

(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
2014年7月24日(24.07.2014)



(10) 国際公開番号
WO 2014/112550 A1

- (51) 国際特許分類:
H04L 9/32 (2006.01)
- (21) 国際出願番号: PCT/JP2014/050651
- (22) 国際出願日: 2014年1月16日(16.01.2014)
- (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 2013-006692 2013年1月17日(17.01.2013) JP
- (71) 出願人: 日本電信電話株式会社(NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).
- (72) 発明者: 五十嵐 大(IKARASHI, Dai); 〒1808585 東京都武蔵野市緑町三丁目9番11号 NTT 知的財産センタ内 Tokyo (JP). 菊池 亮(KIKUCHI, Ryō); 〒1808585 東京都武蔵野市緑町三丁目9番11号 NTT 知的財産センタ内 Tokyo

(JP). 濱田 浩気(HAMADA, Koki); 〒1808585 東京都武蔵野市緑町三丁目9番11号 NTT 知的財産センタ内 Tokyo (JP). 千田 浩司(CHIDA, Koji); 〒1808585 東京都武蔵野市緑町三丁目9番11号 NTT 知的財産センタ内 Tokyo (JP).

(74) 代理人: 中尾 直樹, 外(NAKAO, Naoki et al.); 〒1600022 東京都新宿区新宿三丁目1番22号 新宿NSビル4階 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, BN, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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.

[続葉有]

(54) Title: TAMPERING DETECTION DEVICE, TAMPERING DETECTION METHOD, AND PROGRAM

(54) 発明の名称: 改ざん検知装置、改ざん検知方法、およびプログラム

$$f(\vec{x}, \vec{y}) = \sum_{j,k < q} \alpha_{0,j,k} x_j y_k, \dots, \sum_{j,k < q} \alpha_{q-1,j,k} x_j y_k$$

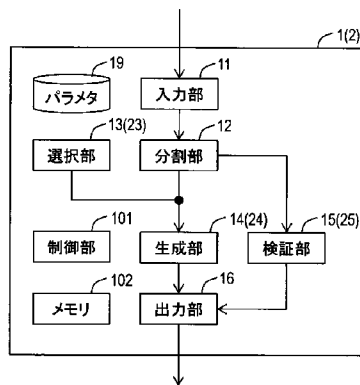


図1

- 11 Input unit
12 Partitioning unit
13(23) Selection unit
14(24) Generation unit
15(25) Validation unit
16 Output unit
19 Parameters
101 Control unit
102 Memory

(57) Abstract: The present invention can be efficiently applied to secure computation and can reduce the success probability of tampering. This tampering detection device contains the following: a parameter storage unit that stores parameters ($\alpha_{i,j,k}$, with $i = 0, \dots, q-1$; $j = 0, \dots, q-1$; and $k = 0, \dots, q-1$) that create a uniform correspondence from one ring (R) to another ring (R^q); a partitioning unit (12) that partitions N values ($a_0, \dots, a_{N-1}$) into vectors ($A_0, \dots, A_{p-1}$) of q values each, starting from a_0 ; a generation unit (13) that uses said vectors ($A_0, \dots, A_{p-1}$) to generate a checksum (c) comprising addition and multiplication, using the function (f) defined by the below formula for vector multiplication; and a validation unit that determines whether or not any of the N values ($a_0, \dots, a_{N-1}$) have been tampered with by comparing the checksum (c) with a validation value generated using the above vectors ($A_0, \dots, A_{p-1}$), using the function (f) defined by the below formula for vector multiplication. N and q are each integers greater than or equal to 2, and p is the smallest integer greater than or equal to N/q .

(57) 要約: 秘匿計算に効率よく適用でき、改ざん成功確率をより低く設定できる。改ざん検知装置は、環 R から環 R^q へ一様に対応させるためのパラメータ $\alpha_{i,j,k}$ ($i=0,\dots,q-1$; $j=0,\dots,q-1$; $k=0,\dots,q-1$) を記憶するパラメータ記憶部と、 N 個の値 $a_0,\dots,a_{N-1}$ を先頭から q 個ずつに分割して値ベクトル $A_0,\dots,A_{p-1}$ を生成する分割部 12 と、値ベクトル $A_0,\dots,A_{p-1}$ を用いて、ベクトルの乗算を下記の式で定義される関数 f として、加算と乗算からなるチェックサム c を生成する生成部 13 と、ベクトルの乗算を下記の式で定義される関数 f として、値ベクトル $A_0,\dots,A_{p-1}$ を用いて生成した検証値とチェックサム c とを比較することで値 $a_0,\dots,a_{N-1}$ のいずれかが改ざんされたか否かを検証する検証部とを含む。ただし、 N, q を 2 以上の整数とし、 p を N/q 以上の最小の整数とする。



(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, KM, ML, MR, NE, SN, TD, TG).

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：

改ざん検知装置、改ざん検知方法、およびプログラム

技術分野

[0001] この発明は、データを秘匿しつつデータ処理を行う秘匿計算においてデータ改ざんを検知するための改ざん検知技術に関する。

背景技術

[0002] 従来の改ざん検知に使用するチェックサムとして非特許文献1に記載の技術がある。非特許文献1に記載のチェックサムは加算と乗算から構成されており秘匿計算に効率よく適用できる。

[0003] 非特許文献1に記載のチェックサムは、 F を体として、値 $a_0, \dots, a_{N-1} \in F$ のチェックサム c を、乱数 $r \in F$ を用いて、以下の式(1)により生成する。

[0004] [数1]

$$c := \sum_{0 \leq i < N} a_i r^{i+1} \quad (1)$$

[0005] 非特許文献1では、以下の式(2)によりチェックサム c を検証する。

[0006] [数2]

$$\sum_{0 \leq i < N} a_i r^{i+1} - c \quad (2)$$

[0007] 式(2)が0であれば、値 $a_0, \dots, a_{N-1}$ はいずれも改ざんされていないと判断する。式(2)が0以外であれば、値 $a_0, \dots, a_{N-1}$ は少なくとも1個が改ざんされていると判断する。

先行技術文献

非特許文献

[0008] 非特許文献1：S. Obana and T. Araki, “Almost optimum secret sharing schemes secure against cheating for arbitrary secret distribution”, A SIACRYPT, Vol. 4284 of Lecture Notes in Computer Science, pp. 364-379

, 2006.

発明の概要

発明が解決しようとする課題

[0009] 非特許文献 1 に記載の改ざん検知技術では、体 F が予め決定されている際の改ざん成功確率は $N/|F|$ である。ここで、 N はチェックサム生成の対象データ数を表し、 $|\cdot|$ は $\cdot$ の要素数を表す。このように、改ざん成功確率がデータ数 N に比例してしまうため、チェックサムを生成する対象データが大きいほど改ざん成功確率が大きくなってしまう。

[0010] この発明の目的は、秘匿計算に効率よく適用でき、改ざん成功確率をより低く設定できる改ざん検知技術を提供することである。

課題を解決するための手段

[0011] 上記の課題を解決するために、この発明の改ざん検知装置は、 N, q を 2 以上の整数とし、 ρ を N/q 以上の最小の整数とし、環 R から環 R^q へ一様に対応させるためのパラメタ $\alpha_{i,j,k}$ ($i=0, \dots, q-1$; $j=0, \dots, q-1$; $k=0, \dots, q-1$) を記憶するパラメタ記憶部と、 N 個の値 $a_0, \dots, a_{N-1}$ を先頭から q 個ずつに分割して値ベクトル $A_0, \dots, A_{\rho-1}$ を生成する分割部と、値ベクトル $A_0, \dots, A_{\rho-1}$ を用いて、ベクトルの乗算を下記の式で定義される関数 f として、加算と乗算からなるチェックサム c を生成する生成部と、ベクトルの乗算を関数 f として、値ベクトル $A_0, \dots, A_{\rho-1}$ を用いて生成した検証値とチェックサム c とを比較することで値 $a_0, \dots, a_{N-1}$ のいずれかが改ざんされたか否かを検証する検証部とを含む。

[0012] [数3]

$$f(\vec{x}, \vec{y}) := \sum_{j,k < q} \alpha_{0,j,k} x_j y_k, \dots, \sum_{j,k < q} \alpha_{q-1,j,k} x_j y_k$$

発明の効果

[0013] この発明の改ざん検知技術によれば、秘匿計算に効率よく適用でき、改ざん成功確率をより低く設定できる。

図面の簡単な説明

[0014] [図1]改ざん検知装置の機能構成を例示する図である。

[図2]チェックサム生成の処理フローを例示する図である。

[図3]チェックサム検証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

[0015] 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。

[0016] [第一実施形態]

この発明の第一実施形態は、非特許文献1に記載の加算と乗算からなるチェックサムに適用した実施形態である。

[0017] <構成>

図1を参照して、この実施形態の改ざん検知装置1の構成例を説明する。改ざん検知装置1は、制御部101、メモリ102、入力部11、分割部12、選択部13、生成部14、検証部15、出力部16、パラメタ記憶部19を備える。改ざん検知装置1は、例えば、CPU (Central Processing Unit)、RAM (Random Access Memory)等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。改ざん検知装置1は制御部101の制御のもとで各処理を実行する。改ざん検知装置1に入力されたデータや各処理で得られたデータはメモリ102に格納され、メモリ102に格納されたデータは必要に応じて読み出されて他の処理に利用される。パラメタ記憶部19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などの半導体メモリ素子により構成される補助記憶装置、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、などにより構成することができる。

[0018] <チェックサム生成処理>

図2を参照して、この実施形態の改ざん検知装置1が実行するチェックサム生成処理の動作例について手続きの順に従って詳細に説明する。以降の説明では、 N, q を2以上の整数とし、 p を N/q 以上の最小の整数とし、 R を環とす

る。

[0019] パラメタ記憶部 19 には、予め環 R から環 R^q へ一様に対応させるためのパラメタ $\alpha_{i,j,k}$ ($i=0, \dots, q-1$; $j=0, \dots, q-1$; $k=0, \dots, q-1$) が記憶されている。パラメタ $\alpha_{i,j,k}$ は環 R と次数 q を決定することで求めることができる。パラメタ $\alpha_{i,j,k}$ は複数の種類があり得るが、計算の容易さなどを考慮して、パラメタ $\alpha_{i,j,k}$ に含まれる q^3 個の値に0が最も多く含まれるものをパラメタ $\alpha_{i,j,k}$ として選択することが望ましい。例えば、 R が体であり、 R^q が体 R の拡大体となるようにパラメタ $\alpha_{i,j,k}$ を決定すれば、効率的に改ざん検知が可能となる。

[0020] 改ざん検知装置 1 の備える入力部 11 へ N 個の値 $a_0, \dots, a_{N-1} \in R$ が入力される（ステップ S 11 a）。入力された値 $a_0, \dots, a_{N-1}$ は分割部 12 へ入力される。値 $a_0, \dots, a_{N-1}$ はどのような情報であってもよいが、例えば準同型暗号の暗号文もしくは秘密分散の分散値などとすることができる。準同型暗号とは準同型性を有するような暗号方式であり、暗号文から暗号化されたままで元の平文の和または積を計算できる暗号方式である。準同型暗号の一例は ElGamal 暗号である。ElGamal 暗号についての詳細は「T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Transactions on Information Theory, vol.31, no.4, pp.469-472, 1985.」などに記載されている。秘密分散とは秘匿したいデータを複数の分散値に変換し、一定個数以上の分散値を用いれば元のデータを復元でき、一定個数未満の分散値からは元のデータを一切復元できなくする技術である。秘密分散の一例は Shamir 秘密分散である。Shamir 秘密分散についての詳細は「A. Shamir, “How to share a secret”, Communications of the ACM, vol.22, issue 11, pp. 612-613, 1979.」などに記載されている。

[0021] 分割部 12 は、 N 個の値 $a_0, \dots, a_{N-1}$ を先頭から q 個ずつに分割して ρ 個の値ベクトル $A_0, \dots, A_{\rho-1}$ を生成する（ステップ S 12 a）。生成した値ベクトル $A_0, \dots, A_{\rho-1}$ は生成部 14 へ入力される。分割した際に最後の値ベクトル $A_{\rho-1}$ の要素数が q とならない場合には、要素数が q となるように任意の値でパディングする。例えば、0でパディングするものとして、 $N=11, q=2$ とした場合には、 $a_0, \dots, a$

$_{10}$ を $A_0:=(a_0, a_1)$, $A_1:=(a_2, a_3)$, $A_2:=(a_4, a_5)$, $\dots$, $A_5:=(a_{10}, 0)$ のように分割すればよい。

[0022] 選択部 1 3 は乱数 $r \in R$ を選択する（ステップ S 1 3）。選択した乱数 r は生成部 1 4 へ入力される。選択部 1 3 は、逐一ランダムに乱数 r を選択してもよいし、事前に生成されメモリ 1 0 2 に格納されている複数個の値から所定の規則に従って乱数 r を選択してもよい。また、乱数 r は真の乱数ではなく任意の暗号方式やハッシュ関数などから生成される疑似乱数であってもよい。

[0023] 生成部 1 4 は値ベクトル $A_0, \dots, A_{p-1}$ と乱数 r を用いてチェックサム c を生成する（ステップ S 1 4）。生成したチェックサム c と乱数 r は出力部 1 6 へ入力される。具体的には生成部 1 4 は、以下の式(3)によりチェックサム c を計算する。

[0024] [数4]

$$c := \sum_{0 \leq i < p} A_i r^{i+1} \quad (3)$$

[0025] この際、ベクトルの乗算は、式(4)(5)で定義される関数 f を用いて計算する。

[0026] [数5]

$$f(\vec{x}, \vec{y}) := f_0(\vec{x}, \vec{y}), \dots, f_{q-1}(\vec{x}, \vec{y}) \quad (4)$$

$$f_i(\vec{x}, \vec{y}) := \sum_{j, k < q} \alpha_{i,j,k} x_j y_k \quad (5)$$

[0027] 出力部 1 6 はチェックサム c と乱数 r を出力する（ステップ S 1 6 a）。

<チェックサム検証処理>

図 3 を参照して、この実施形態の改ざん検知装置 1 が実行するチェックサム検証処理の動作例について手続きの順に従って詳細に説明する。

[0028] 改ざん検知装置 1 の備える入力部 1 1 へ N 個の値 $a_0, \dots, a_{N-1} \in R$ と乱数 $r \in R$ とチェックサム c が入力される（ステップ S 1 1 b）。入力された値 $a_0, \dots, a_{N-1}$ は分割部 1 2 へ入力される。入力された乱数 r とチェックサム c は検証部 1 5 へ入力される。

[0029] 分割部 1 2 は、値 $a_0, \dots, a_{N-1}$ を先頭から q 個ずつに分割して値ベクトル $A_0, \dots, A_{p-1}$ を生成する（ステップ S 1 2 b）。分割の方法はチェックサム生成処理における分割部 1 2 の処理と同様である。また、チェックサム生成処理において生成した値ベクトル $A_0, \dots, A_{p-1}$ を記憶しておくように構成することで、ステップ S 1 2 b の処理は省略することができる。

[0030] 検証部 1 5 は値ベクトル $A_0, \dots, A_{p-1}$ と乱数 r とチェックサム c とを用いて、値 $a_0, \dots, a_{N-1}$ のいずれかが改ざんされたか否かを示す検証結果を生成する（ステップ S 1 5）。検証結果は出力部 1 6 へ入力される。

[0031] 具体的には検証部 1 5 は以下の式(6)を評価する。式(6)が 0 であれば値 $a_0, \dots, a_{N-1}$ のいずれも改ざんされていないと判断する。式(6)が 0 以外であれば値 $a_0, \dots, a_{N-1}$ の少なくとも 1 個が改ざんされていると判断する。

[0032] [数6]

$$\sum_{0 \leq i < p} A_i r^{i+1} - c \quad (6)$$

[0033] この際、ベクトルの乗算は、チェックサム生成処理と同様に、式(4)(5)で定義される関数 f を用いて計算する。

[0034] 出力部 1 6 は検証結果を出力する（ステップ S 1 6 b）。

<効果>

非特許文献 1 に記載のチェックサムは、チェックサム生成対象のデータ数が N 、環 R の要素数が p として、改ざん成功確率が高々 N/p である。環 R が固定であり、例えば $p=2$ とすると、改ざん検知はほとんど無力と言ってよい。

[0035] 第一実施形態のチェックサムは、値ベクトル $A_0, \dots, A_{p-1} \in R^q$ を単位に計算することで、改ざん成功確率を低く抑えることができる。例えば、 Z を整数環、 p を素数、 q を 2 以上の整数として、環 R を素体すなわち Z/pZ としたとき、改ざん成功確率は N/p^q 程度とすることができる。したがって、任意に設定できる拡大次数 q により、任意の低い改ざん成功確率を得ることができる。

[0036] [第二実施形態]

この発明の第二実施形態は、非特許文献 1 に記載のチェックサムよりも改

ざん成功確率を低く抑えることができるチェックサムに適用した実施形態である。

[0037] <構成>

図1を参照して、この実施形態の改ざん検知装置2の構成例を説明する。第二実施形態の改ざん検知装置2の構成は、第一実施形態の改ざん検知装置1と同様であるが、選択部と生成部と検証部の処理が異なる。改ざん検知装置2は、制御部101、メモリ102、入力部11、分割部12、選択部23、生成部24、検証部25、出力部16、パラメタ記憶部19を備える。改ざん検知装置2は、例えば、CPU (Central Processing Unit)、RAM (Random Access Memory) 等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。改ざん検知装置2は制御部101の制御のもとで各処理を実行する。改ざん検知装置2に入力されたデータや各処理で得られたデータはメモリ102に格納され、メモリ102に格納されたデータは必要に応じて読み出されて他の処理に利用される。

[0038] <チェックサム生成処理>

図2を参照して、この実施形態の改ざん検知装置2が実行するチェックサム生成処理の動作例について手続きの順に従って詳細に説明する。以降の説明では、 M, N, q を2以上の整数とし、 $M < N$ とし、 ρ を N/q 以上の最小の整数とし、 R を環とする。

[0039] ステップS11aからステップS12aまでの処理は第一実施形態と同様であるので、ここでは説明を省略する。

[0040] この実施形態の選択部23は M 個の乱数 $r_0, \dots, r_{M-1} \in R$ を選択する(ステップS23)。選択した乱数 $r_0, \dots, r_{M-1}$ は生成部24へ入力される。選択部23は、逐一ランダムに M 個の乱数 $r_0, \dots, r_{M-1}$ を選択してもよいし、事前に生成されメモリ102に格納されている複数個の値から所定の規則に従って M 個の乱数 $r_0, \dots, r_{M-1}$ を選択してもよい。

[0041] この実施形態の生成部24は値ベクトル $A_0, \dots, A_{\rho-1}$ と乱数 $r_0, \dots, r_{M-1}$ を用いて

チェックサム c を生成する（ステップS 2 4）。生成したチェックサム c と乱数 $r_0, \dots, r_{M-1}$ は出力部 1 6 へ入力される。具体的には生成部 2 4 は、以下の式(7)によりチェックサム c を計算する。

[0042] [数7]

$$c := \sum_{i < \rho} A_i \prod_{j < M} r_j^{d(i,j)} \quad (7)$$

[0043] この際、ベクトルの乗算は、第一実施形態と同様に、式(4)(5)で定義される関数 f を用いて計算する。

[0044] 式(7)において、関数 $d(i, j)$ は i 番目の値 a_i に対する j 番目の乱数 r_j の次数を決定する関数である。ただし、 i, i' を自然数とし、 $i \neq i'$ として、いずれかの j (ただし $j < M$)で $d(i, j) \neq d(i', j)$ を満たすものとする。すなわち、乱数 $r_0, \dots, r_{M-1}$ の次数の組み合わせが A_i 毎に重複しない組み合わせとなっていなければならない。

[0045] 例えば、 $\rho=3, M=2$ とした場合であれば、 $c=A_0r_0+A_1r_1+A_2r_0r_1$ のように計算すればよい。また、 $\rho=4, M=2$ とした場合であれば、 $c=A_0r_0+A_1r_1+A_2r_0r_1+A_3r_0^2r_1$ のように計算してもよいし、 $c=A_0r_0^2r_1+A_1r_0r_1+A_2r_1+A_3r_0$ のように計算してもよい。

[0046] M は2以上 ρ 未満であればどのような値であってもよいが、 $\log_2 \rho$ を超える最少の整数とすれば、乱数 $r_0, \dots, r_{M-1}$ に対するすべての次数を1以下にすることができるため、最も効率がよい。例えば、 $\rho=7, M=3$ とした場合であれば、 $c=A_0r_0+A_1r_1+A_2r_0r_1+A_3r_2+A_4r_0r_2+A_5r_1r_2+A_6r_0r_1r_2$ のようにすることができ、すべての乱数の次数を1以下とすることができる。

[0047] 出力部 1 6 はチェックサム c と乱数 $r_0, \dots, r_{M-1}$ を出力する（ステップS 1 6 a）。

<チェックサム検証処理>

図3を参照して、この実施形態の改ざん検知装置2が実行するチェックサム検証処理の動作例について手続きの順に従って詳細に説明する。

[0048] ステップS 1 1 bからステップS 1 2 bまでの処理は第一実施形態と同様であるので、ここでは説明を省略する。

[0049] 検証部 25 は値ベクトル $A_0, \dots, A_{p-1}$ と乱数 $r_0, \dots, r_{M-1}$ とチェックサム c とを用いて、値 $a_0, \dots, a_{N-1}$ のいずれかが改ざんされたか否かを示す検証結果を生成する（ステップ S 25）。検証結果は出力部 16 へ入力される。

[0050] 具体的には検証部 25 は以下の式(8)を評価する。式(8)が真であれば値 $a_0, \dots, a_{N-1}$ のいずれも改ざんされていないと判断する。式(8)が偽であれば値 $a_0, \dots, a_{N-1}$ の少なくとも 1 個が改ざんされていると判断する。

[0051] [数8]

$$c = \sum_{i < p} A_i \prod_{j < M} r_j^{d(i,j)} \quad (8)$$

[0052] この際、ベクトルの乗算は、チェックサム生成処理と同様に、式(4)(5)で定義される関数 f を用いて計算する。

[0053] 式(8)において、関数 $d(i, j)$ は式(7)の関数 $d(i, j)$ と同じ関数である。

[0054] 出力部 16 は検証結果を出力する（ステップ S 16 b）。

<効果>

第二実施形態のチェックサムは、値 $a_0, \dots, a_{N-1} \in R$ を単位に計算した場合には、チェックサム生成対象のデータ数が N 、環 R の要素数が p として、改ざん成功確率が高々 $\log N/p$ である。非特許文献 1 に記載のチェックサムよりも低いながら、それでも環 R が固定であり、例えば $p=2$ とすると改ざん検知はほとんど無力と言ってよい。

[0055] 第二実施形態のチェックサムは、値ベクトル $A_0, \dots, A_{p-1} \in R^q$ を単位に計算することで、改ざん成功確率を低く抑えることができる。例えば、 Z を整数環、 p を素数、 q を 2 以上の整数として、環 R を素体すなわち Z/pZ としたとき、改ざん成功確率は $\log N/p^q$ 程度とすることができる。したがって、任意に設定できる拡大次数 q により、任意の低い改ざん成功確率を得ることができる。

[0056] [応用例]

この発明の改ざん検知技術は様々な利用方法が考えられる。例えば、準同型暗号による暗号文や秘密分散による分散データを第三者の管理するサーバに預託する場合が考えられる。このような場合には、サーバに対して悪意あ

る攻撃者が侵入しデータを改ざんする場合、サーバ自体が悪意を持って預託されたデータを改ざんする場合、サーバがマルウェアに感染してデータを改ざんする場合などのリスクが考えられる。預託するデータに対して、この発明によるチェックサムを生成して付与しておくことで、サーバは秘匿されたデータに対して秘匿されたままデータ処理を行うことができ、さらに、データ改ざんも防止することができる。

[0057] [プログラム、記録媒体]

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。上記実施例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。

[0058] また、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。

[0059] 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、半導体メモリ等のようなものでもよい。

[0060] 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。

[0061] 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。

[0062] 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。

請求の範囲

[請求項1]

N, q を2以上の整数とし、 ρ を N/q 以上の最小の整数とし、
 環 R から環 R^q へ一様に対応させるためのパラメタ $\alpha_{i,j,k}$ ($i=0, \dots, q-1$;
 $j=0, \dots, q-1$; $k=0, \dots, q-1$) を記憶するパラメタ記憶部と、
 N 個の値 $a_0, \dots, a_{N-1}$ を先頭から q 個ずつに分割して値ベクトル $A_0, \dots, A_{\rho-1}$ を生成する分割部と、
 前記値ベクトル $A_0, \dots, A_{\rho-1}$ を用いて、ベクトルの乗算を下記の式で
 定義される関数 f として、加算と乗算からなるチェックサム c を生成する生成部と、

[数9]

$$f(\vec{x}, \vec{y}) := \sum_{j,k < q} \alpha_{0,j,k} x_j y_k, \dots, \sum_{j,k < q} \alpha_{q-1,j,k} x_j y_k$$

ベクトルの乗算を上記関数 f として、前記値ベクトル $A_0, \dots, A_{\rho-1}$ を用いて生成した検証値と前記チェックサム c とを比較することで前記値 $a_0, \dots, a_{N-1}$ のいずれかが改ざんされたか否かを検証する検証部と、
 を含む改ざん検知装置。

[請求項2]

請求項1に記載の改ざん検知装置であって、
 乱数 r を選択する選択部を含み、
 前記生成部は、以下の式を計算することで前記チェックサム c を生成し、

[数10]

$$c := \sum_{0 \leq i < \rho} A_i r^{i+1}$$

前記検証部は、以下の式が0であれば前記値 $a_0, \dots, a_{N-1}$ のいずれも改ざんされていないと判断し、以下の式が0以外であれば前記値 $a_0, \dots, a_{N-1}$ の少なくとも1個が改ざんされていると判断する

[数11]

$$\sum_{0 \leq i < \rho} A_i r^{i+1} - c$$

ことを特徴とする改ざん検知装置。

[請求項3]

請求項1に記載の改ざん検知装置であって、

Mを2以上の整数とし、 $M < N$ とし、 i, i' を自然数とし、 $i \neq i'$ とし、 $j < M$ とし、いずれかのjで $d(i, j)$ を $d(i, j) \neq d(i', j)$ である関数とし、M個の乱数 $r_0, \dots, r_{M-1}$ を選択する選択部を含み、

前記生成部は、以下の式を計算することで前記チェックサムcを生成し、

[数12]

$$c := \sum_{i < \rho} A_i \prod_{j < M} r_j^{d(i, j)}$$

前記検証部は、以下の式が真であれば前記値 $a_0, \dots, a_{N-1}$ のいずれも改ざんされていないと判断し、以下の式が偽であれば前記値 $a_0, \dots, a_{N-1}$ の少なくとも1個が改ざんされていると判断する

[数13]

$$c = \sum_{i < \rho} A_i \prod_{j < M} r_j^{d(i, j)}$$

ことを特徴とする改ざん検知装置。

[請求項4]

N, q を2以上の整数とし、 ρ を N/q 以上の最小の整数とし、 $\alpha_{i, j, k}$ ($i = 0, \dots, q-1$; $j = 0, \dots, q-1$; $k = 0, \dots, q-1$) を環Rから環 R^q へ一様に対応させるためのパラメタとし、

分割部が、N個の値 $a_0, \dots, a_{N-1}$ を先頭からq個ずつに分割して値ベクトル $A_0, \dots, A_{\rho-1}$ を生成する分割ステップと、

生成部が、前記値ベクトル $A_0, \dots, A_{\rho-1}$ を用いて、ベクトルの乗算を下記の式で定義される関数fとして、加算と乗算からなるチェックサムcを生成する生成ステップと、

[数14]

$$f(\vec{x}, \vec{y}) := \sum_{j, k < q} \alpha_{0, j, k} x_j y_k, \dots, \sum_{j, k < q} \alpha_{q-1, j, k} x_j y_k$$

検証部が、ベクトルの乗算を上記関数 f として、前記値ベクトル $A_0, \dots, A_{p-1}$ を用いて生成した検証値と前記チェックサム c とを比較することで前記値 $a_0, \dots, a_{N-1}$ のいずれかが改ざんされたか否かを検証する検証ステップと、

を含む改ざん検知方法。

[請求項5] 請求項 1 から 3 のいずれかに記載の改ざん検知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。

[図1]

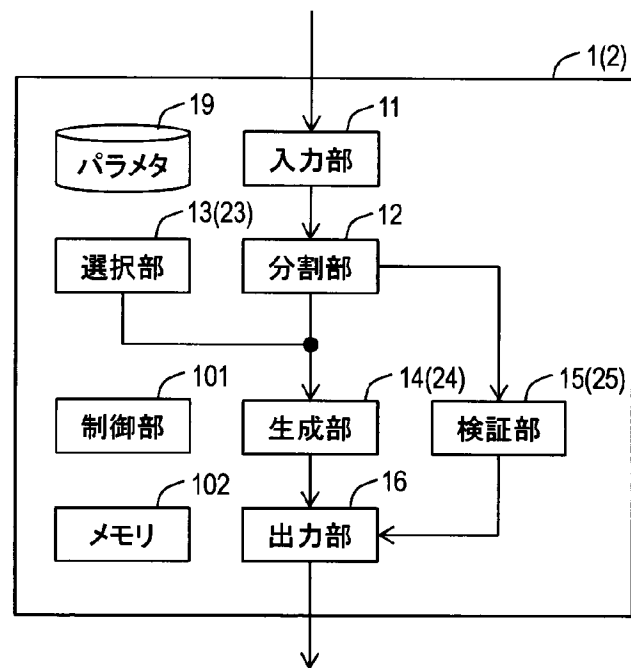


図 1

[図2]

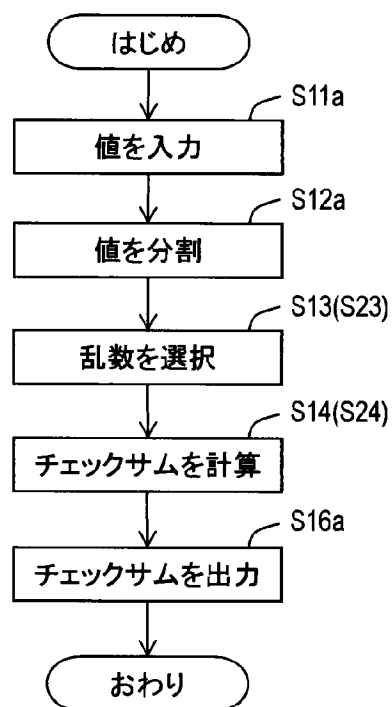


図2

[図3]

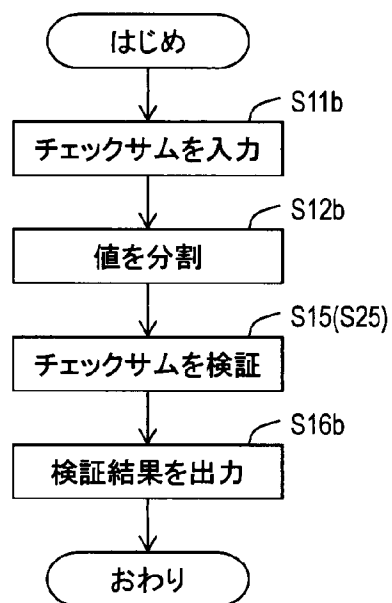


図3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2014/050651

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/32(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)

H04L9/32

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	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JSTPlus/JMEDPlus/JST7580(JDreamIII), secret sharing,
universal hash function

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2008/001628 A1 (NEC Corp.), 03 January 2008 (03.01.2008), paragraphs [0086] to [0095] & JP 5136412 B & US 2009/0204802 A1	1-5
A	Toshinori ARAKI, Satoshi OBANA, "Universal Hash Kansu ni Motozuku Koritsu no Yoi Fusei Kenshutsu Kano na Himitsu Bunsanhu", 2007 Nen Symposium on Cryptography and Information Security Koen Ronbunshu, 23 January 2007 (23. 01.2007), pages 1 to 6	1-5

☐ 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
27 February, 2014 (27.02.14)

Date of mailing of the international search report
11 March, 2014 (11.03.14)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. H04L9/32(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（I P C））

Int.Cl. H04L9/32

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 4 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 4 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 4 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(JDreamIII) secret sharing, universal hash function

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	WO 2008/001628 A1（日本電気株式会社）2008.01.03, 86-95 段落 & JP 5136412 B & US 2009/0204802 A1	1-5
A	荒木俊則, 尾花賢, ユニバーサルハッシュ関数に基づく効率の良い不正検出可能な秘密分散法, 2007年暗号と情報セキュリティシンポジウム講演論文集, 2007.01.23, p. 1-6	1-5

☐ 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

2 7 . 0 2 . 2 0 1 4

国際調査報告の発送日

1 1 . 0 3 . 2 0 1 4

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

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）

中里 裕正

5 S

9 3 6 4

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6