(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
2016 年 6 月 30 日(30.06.2016)

WIPO | PCT

(10) 国際公開番号
WO 2016/104476 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2015/085774

(22) 国際出願日: 2015 年 12 月 22 日(22.12.2015)

(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 2014-264439 2014 年 12 月 26 日(26.12.2014) 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).

(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ＮＳＯビル６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, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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.

(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, ST, 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).

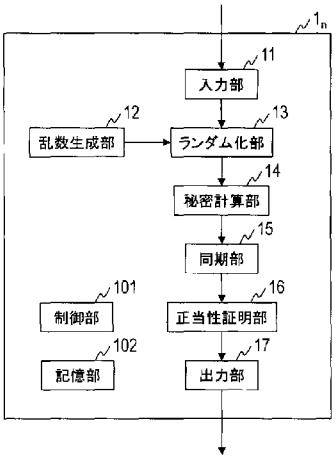
添付公開書類:

— 国際調査報告（条約第 21 条(3)）

(54) **Title**: SECRET FALSIFICATION DETECTION SYSTEM, SECRET CALCULATION DEVICE, SECRET FALSIFICATION DETECTION METHOD, AND PROGRAM

(54) 発明の名称 : 秘密改ざん検知システム、秘密計算装置、秘密改ざん検知方法、およびプログラム

[図2]



11 Input unit
12 Random number generation unit
13 Randomization unit
14 Secret calculation unit
15 Synchronization unit
16 Correctness proving unit
17 Output unit
101 Control unit
102 Storage unit

(57) **Abstract**: The present invention detects falsification during a secret calculation that uses a plurality of secret sharing events. In a secret calculation device 1: sharing values $[a_0],\ldots,[a_{M-1}]$ are set as inputs; function values $[F([a_0],\ldots,[a_{M-1}])]$ are output, the function values being produced by a function F for performing a secret calculation in which J types of secret sharing events are used; and a falsification in a secret calculation is detected. A random number generation unit 12 determines sharing values $[r_0],\ldots,[r_{J-1}]$. A randomization unit 13 calculates a sharing value $[a_m r_j]$ in which a sharing value $[a_m]$ and a sharing value $[r_j]$ are integrated, and generates a randomized sharing value $\langle a_m\rangle:=\langle[a_m],[a_m r_j]\rangle$. A secret calculation unit 14 determines function values $[F([a_0],\ldots,[a_{M-1}])]$ while including the randomized sharing values of the object of calculation and the result of calculation in a checksum C_j. A synchronization unit 15 stands by until the secret calculation that uses all of the secret sharing events is terminated. A correctness proving unit 16 verifies whether the following two values are identical: a sharing value $[\varphi_j]$ obtained by multiplying the sum total of the sharing values $[f_0],\ldots,[f_{\mu j-1}]$ included in the checksum C_j by a sharing value $[r_j]$, and a sharing value $[\psi_j]$ that is the sum total of the sharing values $[f_0 r_j],\ldots,[f_{\mu j-1} r_j]$ included in the checksum C_j.

(57) 要約:

[続葉有]

WO 2016/104476 A1

複数の秘密分散を使用する秘密計算中の改ざんを検知する。秘密計算装置１は、分散値$[a_0],\ldots,[a_{M-1}]$を入力とし、J種類の秘密分散を使う秘密計算を行う関数Fによる関数値$[F([a_0],\ldots,[a_{M-1}])]$を出力とし、秘密計算中の改ざんを検知する。乱数生成部１２は分散値$[r_0],\ldots,[r_{J-1}]$を求める。ランダム化部１３は分散値$[a_m]$と分散値$[r_j]$とを積算した分散値$[a_m r_j]$を計算し、ランダム化分散値$<a_m>:=<[a_m],[a_m r_j]>$を生成する。秘密計算部１４は計算対象と計算結果のランダム化分散値をチェックサムC_jへ含めながら関数値$[F([a_0],\ldots,[a_{M-1}])]$を求める。同期部１５はすべての秘密分散を使う秘密計算が終了するまで待機する。正当性証明部１６は、チェックサムC_jに含まれる分散値$[f_0],\ldots,[f_{\mu j-1}]$の総和に分散値$[r_j]$を乗じた分散値$[\varphi_j]$と、チェックサム$C_j$に含まれる分散値$[f_0 r_j],\ldots,[f_{\mu j-1} r_j]$の総和である分散値$[\psi_j]$とが等しいか否かを検証する。

明　細　書

発明の名称 ：

秘密改ざん検知システム、秘密計算装置、秘密改ざん検知方法、およびプログラム

技術分野

[0001] この発明は、秘密計算技術に関し、特に秘密計算中の改ざんを検知する技術に関する。

背景技術

[0002] 秘密計算中の改ざんを検知する従来技術として、非特許文献１に記載の方法がある。非特許文献１に記載の秘密改ざん検知方法では、環R上の加算・定数倍・乗算・積和・ランダム置換から構成されるm入力μ出力の関数Fを秘匿性および正当性をもつmaliciousモデル上で計算する。なお、maliciousモデルとは、攻撃者が任意の不正な動作を行うモデルである。対してsemi-honestモデルは、攻撃者の行う処理は正しく、その範疇でデータを盗み見ようとするモデルである。

[0003] 非特許文献１では、３つのフェーズで秘密計算中の改ざん検知を行う。ランダム化フェーズでは、分散値を正当性検証可能なランダム化分散値へと変換する。計算フェーズでは、semi-honestの演算により構成されるランダム化分散値用の演算を用いて所望の秘密計算を実行する。このとき、後続の正当性証明フェーズで必要となるチェックサムを収集しながら計算が行われる。正当性証明フェーズでは、計算フェーズで収集されたチェックサムに対して、一括で正当性証明を行う。正当であれば計算フェーズによる計算結果を出力し、正当でなければ計算結果は出力せずに正当でない旨のみを出力する。

先行技術文献

非特許文献

[0004] 非特許文献1：五十嵐大、千田浩司、濱田浩気、菊池亮、“非常に高効率なn≧2k-1 malicious モデル上秘密分散ベースマルチパーティ計算の構成法”、

SCIS2013、2013年

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に記載の秘密改ざん検知技術では、１つの秘密分散を使用する秘密計算を前提としており、複数の秘密分散を使用する秘密計算には適用することができなかった。

[0006] この発明の目的は、このような点に鑑みて、複数の秘密分散を使用する秘密計算中の改ざんを検知することである。

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、この発明の秘密改ざん検知方法は、N台の秘密計算装置が、M個の値$a_0,\cdots,a_{M-1}$を秘密分散した分散値$[a_0],\cdots,[a_{M-1}]$を入力とし、J種類の秘密分散を使う秘密計算を行う関数Fによる関数値$[F([a_0],\cdots,[a_{M-1}])]$を出力とし、秘密計算中の改ざんを検知する秘密改ざん検知方法であって、Nを3以上の整数とし、Mを1以上の整数とし、μを1以上の整数とし、Jを2以上の整数とし、mを0以上M未満の整数とし、jを0以上J未満の整数とし、秘密計算装置の乱数生成部が、J個の乱数$r_0,\cdots,r_{J-1}$を秘密分散した分散値$[r_0],\cdots,[r_{J-1}]$を求める乱数生成ステップと、秘密計算装置のランダム化部が、m番目の分散値$[a_m]$がj番目の秘密分散の分散値であるとし、分散値$[a_m]$と分散値$[r_j]$とを積算した分散値$[a_m r_j]$を計算し、分散値$[a_m]$と分散値$[a_m r_j]$とを組としたランダム化分散値$\langle a_m\rangle:=\langle[a_m],[a_m r_j]\rangle$を生成するランダム化ステップと、秘密計算装置の秘密計算部が、j番目の秘密分散を用いる秘密計算を行う際に、計算対象のランダム化分散値と計算結果のランダム化分散値をチェックサムC_jへ含めながら、関数値$[F([a_0],\cdots,[a_{M-1}])]$を求める秘密計算ステップと、秘密計算装置の同期部が、すべての秘密分散を使う秘密計算が終了するまで待機する同期ステップと、秘密計算装置の正当性証明部が、j=0,…,J-1について、μ_jをj番目のチェックサムC_jに含まれるランダム化分散値の総数とし、$\langle f_0\rangle,\cdots,\langle f_{\mu j-1}\rangle$をj番目のチェックサム$C_j$に含まれるランダム化分散値とし、チェックサム$C_j:=(\langle f_0\rangle,\cdots,\langle f_{\mu j-1}\rangle)$に含まれる分散値$[f_0],\cdots,[f_{\mu j-1}]$の総和に分散値$[r_j]$を乗

じた分散値[ϕ_j]と、チェックサム$C_j:=(\langle f_0\rangle,\cdots,\langle f_{\mu j-1}\rangle)$に含まれる分散値[$f_0 r_j$],…,[$f_{\mu j-1} r_j$]の総和である分散値[$\phi_j$]とが等しいか否かを検証する正当性証明ステップと、を含む。

発明の効果

[0008] この発明の秘密改ざん検知技術によれば、複数の秘密分散を使用する秘密計算中の改ざんを検知できる。

図面の簡単な説明

[0009] [図1]図１は、秘密改ざん検知システムの機能構成を例示する図である。

[図2]図２は、秘密計算装置の機能構成を例示する図である。

[図3]図３は、秘密改ざん検知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

[0010] 実施形態の説明に先立ち、この明細書における表記方法およびこの発明の基本的な考え方について説明する。

[0011] ［表記方法］

この発明で扱う値は、特に断りのない限り環R上の値とする。Aは環R上の結合多元環である。結合多元環とは、結合的な環であって、かつそれと両立するような、何らかの体上の線型空間の構造を備えたものである。結合多元環は、ベクトル空間で扱う値が体ではなく環でよくなったものと言える。

[0012] ベクトルXの第i要素をX_i（下付き添字）で参照する。

[0013] [x]は値x∈Rの秘匿文である。秘匿文は値を暗号化や秘密分散などの手段で秘匿化した値である。Xが集合である場合には、[X]は集合Xの各要素を秘匿化した集合である。

[0014] |X|は集合Xの要素数である。

[0015] ⟨x⟩は値x∈Rのランダム化分散値である。ランダム化分散値とは、値x∈Rの分散値[x]と、値xと乱数r∈Aとの積算値xrの分散値[xr]との組である。したがって、ランダム化分散値は式（１）のように定義できる。

[0016] [数1]

$$\langle x\rangle := ([x],[xr]) \in [\mathrm{R}]\times[\mathrm{A}] \qquad (1)$$

[0017] ランダム化分散値の第０成分（式（１）における[x]）はR成分、第１成分（式（１）における[xr]）はA成分とも呼ぶ。

[0018] 乱数r∈Aをパラメータとするランダム化分散値の空間を<Rr>とする。

[0019] ［安全性］

暗号理論の技術分野ではプロトコルの安全性を証明するために利用者・参加者や攻撃者をモデル化する。このようなモデルとして、maliciousモデルやsemi-honestモデルが用いられている。maliciousモデルは攻撃者が任意の不正な動作を行う。semi-honestモデルは攻撃者の行う処理は正しく、その範疇でデータを盗み見ようとする。したがって、maliciousモデルにおいて安全性が証明されたプロトコルの方がより安全性が高いと評価できる。

[0020] ［発明のポイント］

従来の秘密改ざん検知技術では、一つの秘密分散を使用する秘密計算しか対応できず、複数の秘密分散を使用する秘密計算では改ざん検知ができなかった。複数の秘密分散を使用する場合、秘密分散ごとに従来の秘密改ざん検知技術を用いて個別に検証すればよいようにも思えるが、そのような実装では安全性の問題がある。この発明では、複数の秘密分散を使用する秘密計算において適切な安全性を確保するために、以下の条件を満たすように構成する。

１．同じ環上の秘密分散ではランダム化分散値を生成する際の乱数の値が一致している。

２．正当性検証を行う前にすべての秘密分散において秘密計算が完了している。

[0021] また、各秘密分散を個別に検証するよりも、可能な限りまとめて検証を行う方が公開される値が少なくなるため秘匿性が向上する。そこで、同じ環上の秘密分散では、チェックサムの秘密分散形式を統一し、まとめて検証を行うように構成する。

[0022] ［実施形態］

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。

[0023] 図１を参照して、実施形態の秘密改ざん検知システムの構成例を説明する。秘密改ざん検知システムは、N（≧3）台の秘密計算装置1_1,…,1_Nを含む。本形態では、秘密計算装置1_1,…,1_N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、秘密計算装置1_1,…,1_N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秘密計算装置1_1,…,1_Nへオフラインで入力するように構成してもよい。

[0024] 図２を参照して、秘密改ざん検知システムに含まれる秘密計算装置1_n（n=1,…,N）の構成例を説明する。秘密計算装置1_nは、例えば、制御部１０１、記憶部１０２、入力部１１、乱数生成部１２、ランダム化部１３、秘密計算部１４、同期部１５、正当性証明部１６、および出力部１７を含む。

[0025] 秘密計算装置1_n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。秘密計算装置1_nは、例えば、制御部１０１の制御のもとで各処理を実行する。秘密計算装置1_n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、記憶部１０２に格納され、記憶部１０２に格納されたデータは必要に応じて制御部１０１へ読み出されて他の処理に利用される。秘密計算装置1_n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。

[0026] 図３を参照して、実施形態の秘密改ざん検知方法の処理手続きを説明する。

[0027] ステップＳ１１において、秘密計算装置1_nの入力部１１へM（≧1）個の分散値$[a_0],\cdots,[a_{M-1}]$が入力される。入力された分散値$[a_0],\cdots,[a_{M-1}]$はランダム

化部１３へ出力される。分散値$[a_m]$（m=0,…,M-1）は、値a_mを秘密分散した分散値である。入力される分散値$[a_0],…,[a_{M-1}]$の個数Mは、秘密計算部１４で行われる秘密計算の内容により適宜決定される。

[0028] 秘密分散の方法は、秘密計算上で所望の演算が可能な秘密分散方式であればどのような秘密分散方式であってもよい。本形態の分散値$[a_0],…,[a_{M-1}]$はJ（≧2）種類の秘密分散による分散値が混在していることを前提とする。また、複数の秘密分散は同一の環上の秘密分散であってもよいし、異なる環上の秘密分散であってもよい。また、同一の環上の複数の秘密分散と異なる環上の秘密分散とが混在していてもよい。なお、分散値$[a_0],…,[a_{M-1}]$が、入力時には1種類の秘密分散による分散値のみであり、秘密計算の中で形式変換を行うなどにより、全体として複数の秘密分散が利用されている場合であっても、この発明の改ざん検知技術は適用可能である。適用可能な秘密分散方法についての詳細は、下記参考文献１などを参照されたい。

〔参考文献１〕千田浩司、濱田浩気、五十嵐大、高橋克己、“軽量検証可能３パーティ秘匿関数計算の再考”、CSS2010、2010年

[0029] ステップＳ１２において、乱数生成部１２は、結合多元環Aから選択したJ個の乱数$r_0,…,r_{J-1}∈A$の分散値$[r_0],…,[r_{J-1}]$を生成する。生成した分散値$[r_0],…,[r_{J-1}]$はランダム化部１３に出力される。分散値$[r_0],…,[r_{J-1}]$の生成は、いずれの秘密計算装置$1_1,…,1_N$からも乱数$r_0,…,r_{J-1}$が秘匿された状態で行われなければならない。

[0030] 例えば、秘密改ざん検知システムを構成する秘密計算装置$1_1,…,1_N$が協調して乱数r_jの分散値$[r_j]$を生成することができる。具体的には、まず、秘密計算装置1_nはそれぞれが乱数r_nを生成する。次に、上記の参考文献１に記載された秘匿方法により乱数r_nの分散値$[r_n]$を生成する。そして、秘密計算装置1_nはそれぞれ$[r_j]=Σ_{n<N}[r_n]$を計算し、乱数r_jの分散値$[r_j]$を得る。このように構成すれば、いずれの秘密計算装置$1_1,…,1_N$も乱数r_jを知ることなく、乱数r_jの分散値$[r_j]$を得ることができる。また、事前の乱数共有や疑似乱数の利用を許すことが可能であれば、複製型秘密分散（replicated secret sharing）を

利用して乱数r_jの分散値$[r_j]$を生成することができる。複製型秘密分散を利用すれば秘密計算装置$1_1,\cdots,1_N$間での通信なしに乱数r_jの分散値$[r_j]$を生成することができる。複製型秘密分散の詳細については、下記参考文献２を参照されたい。

〔参考文献２〕R. Cramer, I. Damgard, and Y. Ishai, “Share conversion, pseudorandom secret-sharing and applications to secure computation”, TCC, Vol. 3378 of Lecture Notes in Computer Science, pp. 342-362, Springer, 2005.

[0031] J個の秘密分散のうち同一の環上の秘密分散が存在する場合には、一方の秘密分散のための分散値を他方の秘密分散のための分散値に変換することで、乱数の値が同一となるように生成する。この形式変換においても、改ざん検知が可能もしくは改ざんが不可能でなければならない。例えば、j（$j=0,\cdots,J-1$）番目の秘密分散とj’（$j'=0,\cdots,J-1$、$j\neq j'$）番目の秘密分散が同一の環上の秘密分散である場合には、j番目の秘密分散のための乱数r_jを秘密分散した分散値$[r_j]$を生成し、その分散値$[r_j]$を改ざん検知可能もしくは改ざん不可能な方法によりj’番目の秘密分散による分散値$[r_{j'}]$に形式変換する。例えば、複製型秘密分散から線形秘密分散（linear secret sharing）へ変換する改ざん不可能な方法は、上記参考文献２に記載されている。

[0032] ステップＳ１３において、ランダム化部１３は、分散値$[a_0],\cdots,[a_{M-1}]$と分散値$[r_0],\cdots,[r_{J-1}]$とを用いて、ランダム化分散値$\langle a_0\rangle,\cdots,\langle a_{M-1}\rangle$を生成する。具体的には、ランダム化部１３は、$m=0,\cdots,M-1$について、m番目の分散値$[a_m]$がj番目の秘密分散による分散値であるとして、分散値$[a_m]$と分散値$[r_j]$とを用いて、$[a_m r_j]=[a_m]\times[r_j]$を上記参考文献１に記載された秘密計算方法により求め、分散値$[a_m]$と分散値$[a_m r_j]$とを組としてランダム化分散値$\langle a_m\rangle=([a_m],[a_m r_j])$を生成する。生成したランダム化分散値$\langle a_0\rangle,\cdots,\langle a_{M-1}\rangle$は秘密計算部１４へ出力される。

[0033] ステップＳ１４において、秘密計算部１４は、ランダム化分散値$\langle a_0\rangle,\cdots,\langle a_{M-1}\rangle$に対して、J種類の秘密分散を使用する秘密計算を実行する関数Fを計算し

て秘匿された関数値[F([a_0],…,[a_{M-1}])]を求める。この際、使用する秘密分散の種類に対応するJ個のチェックサムへ計算対象のランダム化分散値と計算結果のランダム化分散値を含めながら関数Fを計算する。例えば、j（j=0,…,J-1）番目の秘密分散を用いる演算であれば、計算対象のランダム化分散値と計算結果のランダム化分散値をj番目のチェックサムC_j:=<f_0>,…,<$f_{\mu j-1}$>へ追加する。ここで、<f_0>,…,<$f_{\mu j-1}$>は計算対象もしくは計算結果の各ランダム化分散値であり、下付き添え字の「μj-1」はμ_{j-1}を表しており、μ_jはチェックサムC_jに含まれるランダム化分散値の数である。μ_jの値は初期値を0としてチェックサムC_jにランダム化分散値を新たに含めるたびに加算される。チェックサムに含める対象のランダム化分散値やチェックサムにランダム化分散値を取得するべきタイミングは、秘密計算の演算の種類（例えば、加算・定数倍、乗算、積和、ランダム置換など）によって異なる。これらの詳細は、非特許文献１に記載の秘密改ざん検知方法と同様である。

[0034] ステップＳ１５において、同期部１５は、正当性証明を行う前に、すべての秘密分散についてすべての秘密計算が終了するまで待機する同期処理（SYNC）を実行する。同期部１５は、すべての秘密分散についてすべての秘密計算が終了したことを検知すると、秘密計算部１４により求められた関数値[F([a_0],…,[a_{M-1}])]と、J個のチェックサムC_0,…,C_{J-1}を正当性証明部１６へ出力する。

[0035] ステップＳ１６において、正当性証明部１６は、分散値[r_0],…,[r_{J-1}]を用いてチェックサムC_0,…,C_{J-1}を検証することで、関数値[F([a_0],…,[a_{M-1}])]の正当性を証明する。J個のチェックサムC_0,…,C_{J-1}すべてを検証した結果、改ざんがないと判定した場合は関数値[F([a_0],…,[a_{M-1}])]を出力部１７へ出力する。改ざんがあったと判断した場合はその旨を示す情報（例えば、「⊥」など）を出力部１７へ出力する。

[0036] ステップＳ１６において改ざんがないと判定した場合であって、所望の関数を計算するための後続の処理が残されている場合には、再度ステップＳ１４に戻り、秘密計算から正当性証明まで処理を繰り返し実行してもよい。こ

の際、正当性証明が完了するたびに、チェックサム$C_0,\cdots,C_{J-1}$に含まれるランダム化分散値を破棄してもよい。このような秘密計算と正当性証明の繰り返しは、改ざんされていないことが保証された値を公開し、その値を用いて後続の処理を行うような場合に必要となる。改ざんされた値が公開されることは、秘匿性を損なう原因となる場合があるためである。

[0037] ステップＳ１７において、出力部１７は、正当性証明部１６から受け取った関数値$[F([a_0],\cdots,[a_{M-1}])]$もしくは改ざんがあった旨を示す情報を出力する。

[0038] j番目のチェックサムC_jの検証は、チェックサムC_jに含まれるランダム化分散値のR成分$[f_0],\cdots,[f_{\mu j-1}]$の総和に分散値$[r_j]$を乗じた分散値$[\phi_j]$と、チェックサム$C_j$に含まれるランダム化分散値のA成分$[f_0 r_j],\cdots,[f_{\mu j-1} r_j]$の総和である分散値$[\phi_j]$とに基づいて行われる。具体的には、正当性証明部１６は、例えば、以下のようにしてチェックサムC_jを検証する。まず、結合多元環A上のμ_j個の乱数$\rho_0,\cdots,\rho_{\mu j-1}$の分散値$[\rho_0],\cdots,[\rho_{\mu j-1}]$を生成する。分散値$[\rho_0],\cdots,[\rho_{\mu j-1}]$の生成はいずれの秘密計算装置$1_n$からも乱数$\rho_0,\cdots,\rho_{\mu j-1}$が秘匿された状態で行われなければならない。分散値$[\rho_0],\cdots,[\rho_{\mu j-1}]$の生成は、乱数生成部１２と同様の方法により行えばよい。次に、チェックサムC_jに含まれるランダム化分散値のR成分$[f_0],\cdots,[f_{\mu j-1}]$と、乱数$\rho_0,\cdots,\rho_{\mu j-1}$の分散値$[\rho_0],\cdots,[\rho_{\mu j-1}]$と、乱数$r_j$の分散値$[r_j]$とを用いて、以下の式（２）により分散値$[\phi_j]$を求める。

[0039] [数2]

$$[\varphi_j] := \left(\sum_{i<\mu_j} [f_i][\rho_i] \right) [r_j] \qquad (2)$$

[0040] また、チェックサムC_jに含まれるランダム化分散値のA成分$[f_0 r_j],\cdots,[f_{\mu j-1} r_j]$と、乱数$\rho_0,\cdots,\rho_{\mu j-1}$の分散値$[\rho_0],\cdots,[\rho_{\mu j-1}]$とを用いて、以下の式（３）により分散値$[\phi_j]$を求める。

[0041]

[数3]

$$[\psi_j] := \sum_{i<\mu_j} [f_i r_j][\rho_i] \qquad (3)$$

[0042] そして、分散値[ϕ_j]と分散値[φ_j]とを減算した分散値[δ_j]=[ϕ_j]-[φ_j]を復元する。復元の方法は、各分散値に対応する秘密分散方式の復元操作で行えばよいが、この際、maliciousモデルで正当性を保証する。具体的にはすべての秘密計算装置1_n（n=0,…,N-1）が互いに分散値[δ_j]を他の秘密計算装置$1_{n'}$（n'=0,…,N-1、n≠n'）へ送信し、分散値の一貫性を確認することで完全な正当性を保証する。この場合、秘密計算装置1_nの総数をNとして、総通信量はN(N-1)である。分散値のデータ量が大きいとき、確率的な方法を用いれば、復元に必要な秘密計算装置1_nの数をKとして、総通信量をN(K-1)とすることができる。なお、秘密計算には正当性を保証しない復元を含むsemi-honest演算もあるが、秘密計算の構成要素として正当性を保証しない復元が含まれていても、秘密計算全体の安全性には影響しない。

[0043] すべての秘密計算装置1_1,…,1_Nにおいて復元した値δ_0,…,δ_{J-1}が0であれば、秘密計算全体を通して改ざんがなかったものと判定する。いずれかの秘密計算装置1_jにおいて復元した値δ_jが0以外であれば、秘密計算において改ざんがあったものと判定する。

[0044] J種類の秘密分散のうち同一の環上の秘密分散が存在する場合には、可能な限りまとめて正当性証明を行うと、公開される値の数が少なくなるため、より秘匿性を向上することができる。例えば、j（j=0,…,J-1）番目の秘密分散とj'（j'=0,…,J-1、j≠j'）番目の秘密分散が同一の環上の秘密分散である場合には、以下のように正当性証明を行う。まず、チェックサムC_jから上述のように算出した分散値[ϕ_j]と、チェックサムC_jから上述のように算出した分散値[φ_j]とをそれぞれj'番目の秘密分散へ変換する。そして、変換後の分散値[ϕ_j]とチェックサム$C_{j'}$から算出した分散値[$\phi_{j'}$]とを合算した分散値[$\phi_j+\phi_{j'}$]と、変換後の分散値[φ_j]とj'番目のチェックサム$C_{j'}$から算出した分散値[$\varphi_{j'}$]とを合算した分散値[$\varphi_j+\varphi_{j'}$]とが等しいか否かを検証する。すなわち、

すべての同じ環上の秘密分散の組み合わせについて、[δ]=([φ$_j$]+[φ$_{j'}$])-([φ$_j$]+[φ$_{j'}$])を計算し、復元値δが0であれば、j番目の秘密分散とj'番目の秘密分散を用いる秘密計算は全体を通して改ざんがなかったものと判定する。[δ]=([φ$_j$]+[φ$_{j'}$])-([φ$_j$]+[φ$_{j'}$])を計算し、復元値δが0以外であれば、j番目の秘密分散とj'番目の秘密分散を用いる秘密計算のいずれかの演算において改ざんがあったものと判定する。このようにして、すべての同一の環上の秘密分散の組み合わせについて検証し、秘密計算全体で改ざんがなかったことを検証する。本形態では２個の秘密分散が同一の環上の秘密分散である例を説明したが、３個以上の秘密分散が同一の環上の秘密分散である場合でも、同様の方法により正当性証明を行うことができる。

[0045] 正当性証明の基本的な考え方を説明する。チェックサムの検証は、ランダム化分散値<f$_i$>それぞれに着目すると、[f$_i$][r$_j$]-[f$_i$r$_j$]=0であるかを検証することである。ここで、分散値[f$_i$]と分散値[f$_i$r$_j$]がいずれも改ざんされ、[f$_i$+x]と[f$_i$r$_j$+y]とされた場合を考えると、検証により得られる値は式（４）となる。

[0046] [数4]

$$[f_i + x][r_j] - [f_i r_j + y] = [xr_j - y] \qquad (4)$$

[0047] 攻撃者はこのxr$_j$-yの値を0となるように辻褄を合わせて[f$_i$]と[f$_i$r$_j$]を操作しなければならないが、攻撃者は乱数r$_j$∈Aを知らないため、これを満たすようにすることができる確率は、1/|A|となる。ただし、本形態では乱数ρ$_0$,…,ρ$_{μj-1}$を乗じているため全体の改ざん成功確率は高々2/|A|となる。

[0048] このようにして、本形態の秘密改ざん検知システムは、複数の秘密分散を用いる秘密計算においても改ざん検知が可能となる。

[0049] 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。

[0050] ［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。

[0051] 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。

[0052] 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、USBメモリ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。

[0053] 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。

[0054] 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台の秘密計算装置が、M個の値$a_0,\cdots,a_{M-1}$を秘密分散した分散値$[a_0],\cdots,[a_{M-1}]$を入力とし、J種類の秘密分散を使う秘密計算を行う関数Fによる関数値$[F([a_0],\cdots,[a_{M-1}])]$を出力とし、秘密計算中の改ざんを検知する秘密改ざん検知方法であって、

Nを3以上の整数とし、Mを1以上の整数とし、μを1以上の整数とし、Jを2以上の整数とし、mを0以上M未満の整数とし、jを0以上J未満の整数とし、

上記秘密計算装置の乱数生成部が、J個の乱数$r_0,\cdots,r_{J-1}$を秘密分散した分散値$[r_0],\cdots,[r_{J-1}]$を求める乱数生成ステップと、

上記秘密計算装置のランダム化部が、m番目の分散値$[a_m]$がj番目の秘密分散の分散値であるとし、上記分散値$[a_m]$と上記分散値$[r_j]$とを積算した分散値$[a_m r_j]$を計算し、上記分散値$[a_m]$と上記分散値$[a_m r_j]$とを組としたランダム化分散値$\langle a_m\rangle:=\langle[a_m],[a_m r_j]\rangle$を生成するランダム化ステップと、

上記秘密計算装置の秘密計算部が、j番目の秘密分散を用いる秘密計算を行う際に、計算対象のランダム化分散値と計算結果のランダム化分散値をチェックサムC_jへ含めながら、上記関数値$[F([a_0],\cdots,[a_{M-1}])]$を求める秘密計算ステップと、

上記秘密計算装置の同期部が、すべての秘密分散を使う秘密計算が終了するまで待機する同期ステップと、

上記秘密計算装置の正当性証明部が、j=0,…,J-1について、μ_jをj番目のチェックサムC_jに含まれるランダム化分散値の総数とし、$\langle f_0\rangle,\cdots,\langle f_{\mu_{j-1}}\rangle$をj番目のチェックサム$C_j$に含まれるランダム化分散値とし、上記チェックサム$C_j:=(\langle f_0\rangle,\cdots,\langle f_{\mu_{j-1}}\rangle)$に含まれる分散値$[f_0],\cdots,[f_{\mu_{j-1}}]$の総和に上記分散値$[r_j]$を乗じた分散値$[\phi_j]$と、上記チェックサム$C_j:=(\langle f_0\rangle,\cdots,\langle f_{\mu_{j-1}}\rangle)$に含まれる分散値$[f_0 r_j],\cdots,[f_{\mu_{j-1}} r_j]$の総和である分散値$[\phi_j]$とが等しいか否かを検証する正当性証明ステップ

と、

を含む秘密改ざん検知方法。

[請求項2] 請求項１に記載の秘密改ざん検知方法であって、

j'を0以上J未満の整数とし、j≠j'とし、j番目の秘密分散とj'番目の秘密分散とが同一の環上の秘密分散であるとし、j番目の秘密分散からj'番目の秘密分散へ改ざん検知可能もしくは改ざん不可能な方式により変換可能であるとし、

上記乱数生成ステップは、乱数r_jをj番目の秘密分散により秘密分散した分散値$[r_j]$を生成し、上記分散値$[r_j]$をj'番目の秘密分散へ変換して分散値$[r_{j'}]$を生成するものである

秘密改ざん検知方法。

[請求項3] 請求項２に記載の秘密改ざん検知方法であって、

上記正当性証明ステップは、j番目のチェックサムC_jから算出した上記分散値$[\phi_j]$と上記チェックサムC_jから算出した上記分散値$[\phi_j]$とをそれぞれj'番目の秘密分散へ変換し、上記分散値$[\phi_j]$とj'番目のチェックサム$C_{j'}$から算出した上記分散値$[\phi_{j'}]$とを合算した分散値$[\phi_j+\phi_{j'}]$と、上記分散値$[\phi_j]$とj'番目のチェックサム$C_{j'}$から算出した上記分散値$[\phi_{j'}]$とを合算した分散値$[\phi_j+\phi_{j'}]$とが等しいか否かを検証するものである

秘密改ざん検知方法。

[請求項4] 請求項１から３のいずれかに記載の秘密改ざん検知方法であって、

上記秘密計算ステップと上記同期ステップと上記正当性証明ステップとを複数回繰り返し実行する

秘密改ざん検知方法。

[請求項5] N台の秘密計算装置が、M個の値$a_0,\cdots,a_{M-1}$を秘密分散した分散値$[a_0],\cdots,[a_{M-1}]$を入力とし、J種類の秘密分散を使う秘密計算を行う関数Fによる関数値$[F([a_0],\cdots,[a_{M-1}])]$を出力とし、秘密計算中の改ざんを検知する秘密改ざん検知システムであって、

Nを3以上の整数とし、Mを1以上の整数とし、μを1以上の整数とし、Jを2以上の整数とし、mを0以上M未満の整数とし、jを0以上J未満の整数とし、

上記秘密計算装置は、

J個の乱数$r_0,\cdots,r_{J-1}$を秘密分散した分散値$[r_0],\cdots,[r_{J-1}]$を求める乱数生成部と、

m番目の分散値$[a_m]$がj番目の秘密分散の分散値であるとし、上記分散値$[a_m]$と上記分散値$[r_j]$とを積算した分散値$[a_m r_j]$を計算し、上記分散値$[a_m]$と上記分散値$[a_m r_j]$とを組としたランダム化分散値$\langle a_m\rangle:=\langle[a_m],[a_m r_j]\rangle$を生成するランダム化部と、

j番目の秘密分散を用いる秘密計算を行う際に、計算対象のランダム化分散値と計算結果のランダム化分散値をチェックサムC_jへ含めながら、上記関数値$[F([a_0],\cdots,[a_{M-1}])]$を求める秘密計算部と、

すべての秘密分散を使う秘密計算が終了するまで待機する同期部と、

j=0,…,J-1について、μ_jをj番目のチェックサムC_jに含まれるランダム化分散値の総数とし、$\langle f_0\rangle,\cdots,\langle f_{\mu j-1}\rangle$をj番目のチェックサム$C_j$に含まれるランダム化分散値とし、上記チェックサム$C_j:=(\langle f_0\rangle,\cdots,\langle f_{\mu j-1}\rangle)$に含まれる分散値$[f_0],\cdots,[f_{\mu j-1}]$の総和に上記分散値$[r_j]$を乗じた分散値$[\phi_j]$と、上記チェックサム$C_j:=(\langle f_0\rangle,\cdots,\langle f_{\mu j-1}\rangle)$に含まれる分散値$[f_0 r_j],\cdots,[f_{\mu j-1} r_j]$の総和である分散値$[\phi_j]$とが等しいか否かを検証する正当性証明部と、

を含む秘密改ざん検知システム。

[請求項6] M個の値$a_0,\cdots,a_{M-1}$を秘密分散した分散値$[a_0],\cdots,[a_{M-1}]$を入力とし、J種類の秘密分散を使う秘密計算を行う関数Fによる関数値$[F([a_0],\cdots,[a_{M-1}])]$を出力とし、秘密計算中の改ざんを検知する秘密計算装置であって、

Nを3以上の整数とし、Mを1以上の整数とし、μを1以上の整数とし

、Jを2以上の整数とし、mを0以上M未満の整数とし、jを0以上J未満の整数とし、

J個の乱数$r_0,\cdots,r_{J-1}$を秘密分散した分散値$[r_0],\cdots,[r_{J-1}]$を求める乱数生成部と、

m番目の分散値$[a_m]$がj番目の秘密分散の分散値であるとし、上記分散値$[a_m]$と上記分散値$[r_j]$とを積算した分散値$[a_m r_j]$を計算し、上記分散値$[a_m]$と上記分散値$[a_m r_j]$とを組としたランダム化分散値$\langle a_m\rangle:=\langle [a_m],[a_m r_j]\rangle$を生成するランダム化部と、

j番目の秘密分散を用いる秘密計算を行う際に、計算対象のランダム化分散値と計算結果のランダム化分散値をチェックサムC_jへ含めながら、上記関数値$[F([a_0],\cdots,[a_{M-1}])]$を求める秘密計算部と、

すべての秘密分散を使う秘密計算が終了するまで待機する同期部と、

$j=0,\cdots,J-1$について、μ_jをj番目のチェックサムC_jに含まれるランダム化分散値の総数とし、$\langle f_0\rangle,\cdots,\langle f_{\mu j-1}\rangle$をj番目のチェックサム$C_j$に含まれるランダム化分散値とし、上記チェックサム$C_j:=(\langle f_0\rangle,\cdots,\langle f_{\mu j-1}\rangle)$に含まれる分散値$[f_0],\cdots,[f_{\mu j-1}]$の総和に上記分散値$[r_j]$を乗じた分散値$[\phi_j]$と、上記チェックサム$C_j:=(\langle f_0\rangle,\cdots,\langle f_{\mu j-1}\rangle)$に含まれる分散値$[f_0 r_j],\cdots,[f_{\mu j-1} r_j]$の総和である分散値$[\phi_j]$とが等しいか否かを検証する正当性証明部と、

を含む秘密計算装置。

[請求項7] 請求項６に記載の秘密計算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]

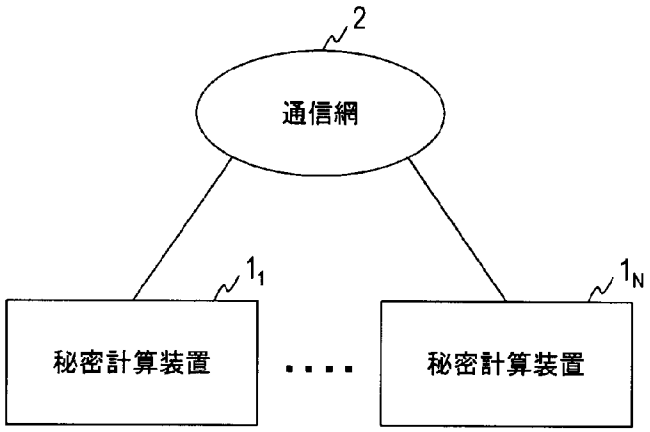

秘密改ざん検知システム
2
通信網
1₁
1N
秘密計算装置
秘密計算装置

図1

[図2]

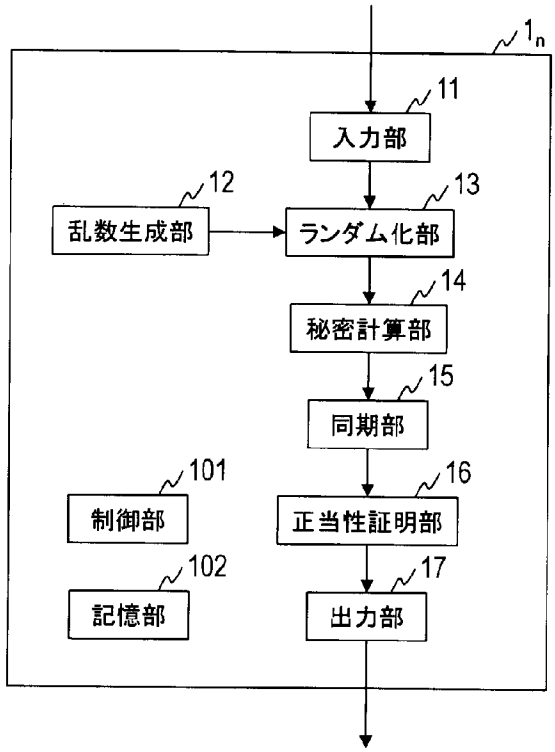

1n
11
入力部
12
乱数生成部
13
ランダム化部
14
秘密計算部
15
同期部
101
制御部
16
正当性証明部
102
記憶部
17
出力部

図2

[図3]

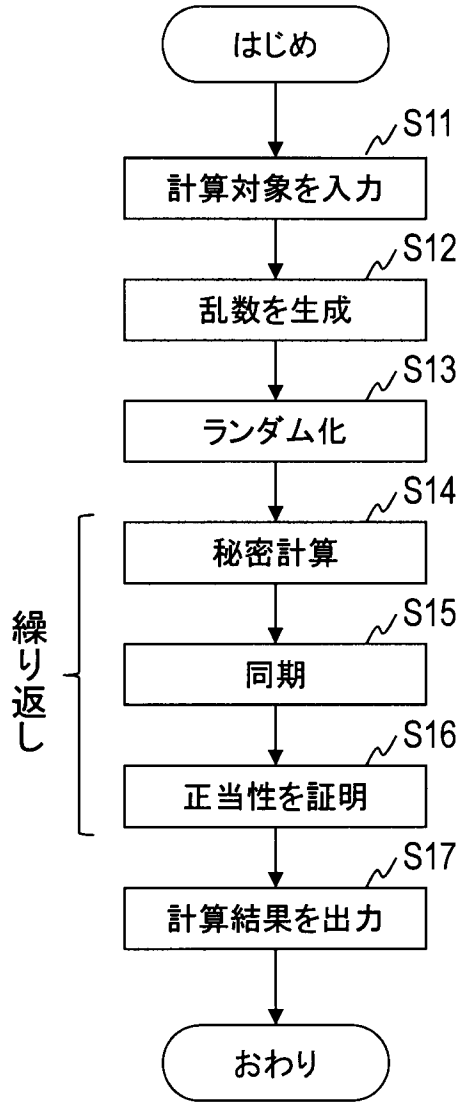

はじめ
S11
計算対象を入力
S12
乱数を生成
S13
ランダム化
S14
秘密計算
S15
同期
S16
正当性を証明
S17
計算結果を出力
おわり
繰り返し

図3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/085774

A. CLASSIFICATION OF SUBJECT MATTER
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)
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 1996-2016
Kokai Jitsuyo Shinan Koho 1971-2016 Toroku Jitsuyo Shinan Koho 1994-2016

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2014/112548 A1 (Nippon Telegraph and Telephone Corp.), 24 July 2014 (24.07.2014), paragraphs [0001] to [0069]; fig. 1, 2 & US 2015/0358155 A1 paragraphs [0001] to [0076]; fig. 1, 2 & EP 2947642 A1 & CN 105027180 A	1-7
A	JP 2013-9245 A (NEC Corp.), 10 January 2013 (10.01.2013), paragraphs [0001] to [0133] (Family: none)	1-7

☒ 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
17 March 2016 (17.03.16)	29 March 2016 (29.03.16)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/085774

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2014-137474 A (Nippon Telegraph and Telephone Corp.), 28 July 2014 (28.07.2014), paragraphs [0001] to [0040] (Family: none)	1-7
A	JP 2014-138349 A (Nippon Telegraph and Telephone Corp.), 28 July 2014 (28.07.2014), paragraphs [0001] to [0124] (Family: none)	1-7
A	IKARASHI,Dai et al., Actively Private and Correct MPC Scheme in t<n/2 from Passively Secure Schemes with Small Overhead, Cryptology ePrint Archive, 2014.04.30, entire text, [online], [retrieval date 2016.03.17], Internet: <URL:https://eprint.iacr.org/2014/304/20140430:210051>	1-7
A	Ryo KIKUCHI et al., "Himitsu Keisan ni Tekishita Himitsu Bunsan to Compact na Himitsu Bunsan tono Sogo Henkan Protocol", 2014 Nen Symposium on Cryptography and Information Security Gaiyoshu, 21 January 2014 (21.01.2014), pages 1 to 8	1-7
A	Dai IKARASHI, "Hijo ni Kokoritsu na n≥2k-1 malicious Model-jo Himitsu Bunsan Base Multi Party Keisan no Koseiho", 2013 Nen Symposium on Cryptography and Information Security Gaiyoshu, 22 January 2013 (22.01.2013), pages 1 to 8	1-7

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１５／０８５７７４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　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.　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	１９７１－２０１６年
日本国実用新案登録公報	１９９６－２０１６年
日本国登録実用新案公報	１９９４－２０１６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）

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 2014/112548 A1（日本電信電話株式会社）2014.07.24，段落［0001］－［0069］，図１，２ & US 2015/0358155 A1，段落［0001］－［0076］，図１，２ & EP 2947642 A1 & CN 105027180 A	1-7
A	JP 2013-9245 A（日本電気株式会社）2013.01.10，段落［0001］－［0133］（ファミリーなし）	1-7

☑　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
１７．０３．２０１６	２９．０３．２０１６

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　６３０４
中里　裕正
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　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	JP 2014-137474 A (日本電信電話株式会社) 2014.07.28, 段落 [0001] － [0040] （ファミリーなし）	1-7
A	JP 2014-138349 A (日本電信電話株式会社) 2014.07.28, 段落 [0001] － [0124] （ファミリーなし）	1-7
A	IKARASHI, Dai et al., Actively Private and Correct MPC Scheme in t<n/2 from Passively Secure Schemes with Small Overhead, Cryptology ePrint Archive, 2014.04.30, 全文, [online], [検索日 2016.03.17], インターネット：<URL:https://eprint.iacr.org/2014/304/20140430:210051>	1-7
A	菊池　亮 ほか, 秘密計算に適した秘密分散とコンパクトな秘密分散との相互変換プロトコル, ２０１４年　暗号と情報セキュリティシンポジウム概要集, 2014.01.21, p.1-8	1-7
A	五十嵐大, 非常に高効率なｎ≧２ｋ－１ｍａｌｉｃｉｏｕｓモデル上秘密分散ベースマルチパーティ計算の構成法, ２０１３年　暗号と情報セキュリティシンポジウム概要集, 2013.01.22, p.1-8	1-7