(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6040320号
(P6040320)

(45)発行日　平成28年12月7日(2016.12.7)　(24)登録日　平成28年11月11日(2016.11.11)

(51)Int.Cl.			F I		
G09C	1/00	(2006.01)	G09C	1/00	650Z
H04L	9/32	(2006.01)	H04L	9/00	675A
			G09C	1/00	640D

請求項の数 9　(全 16 頁)

(21)出願番号	特願2015-541550 (P2015-541550)
(86)(22)出願日	平成26年10月3日 (2014.10.3)
(86)国際出願番号	PCT/JP2014/076531
(87)国際公開番号	WO2015/053184
(87)国際公開日	平成27年4月16日 (2015.4.16)
審査請求日	平成28年3月29日 (2016.3.29)
(31)優先権主張番号	特願2013-213026 (P2013-213026)
(32)優先日	平成25年10月10日 (2013.10.10)
(33)優先権主張国	日本国(JP)

(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
(72)発明者　菊池　亮
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

最終頁に続く

(54)【発明の名称】秘密並列処理装置、秘密並列処理方法、プログラム

(57)【特許請求の範囲】

【請求項１】

入力列である非ランダム化系列を取得して、前記非ランダム化系列と公開値からなるダミーレコード列とを結合してランダム置換処理したランダム化系列と、利用されたランダム置換データを秘匿した秘匿済みランダム置換データを出力するランダム化部と、

前記非ランダム化系列と、前記ランダム化系列と、前記ダミーレコード列を取得して、これらに所定の関数を施して、当該関数を施す処理における計算過程のデータを用いて各系列の出力チェックサムを生成する計算部と、

前記各系列の出力チェックサムと、前記秘匿済みランダム置換データを取得して、前記各系列の出力チェックサムを評価して、前記非ランダム化系列に前記所定の関数が正しく施されたか否かの最終検証結果を出力する正当性証明部と、

を含む秘密並列処理装置。

【請求項２】

請求項１に記載の秘密並列処理装置であって、

平文空間をＲとし、

関数ｆ：Ｒ→Ｒ′に対して、$f^N : R^N \rightarrow R'^N$をｆの並列実行、すなわち

$f^N(a_0, \cdots, a_{N-1}) = (f(a_0), \cdots, f(a_{N-1}))$とし、

環Ｒに対して0_RをＲの零元とし、

Ｘを任意の集合とし、

ｍおよびｍ′を任意の整数とし、

ｉを任意の整数とし、
X^mの元ｘに対して、ｉ番目の要素をx_iと表記し、
$x \in X^m$，$y \in X^{m'}$に対して、結合
$(x_0, \cdots, x_{m-1}, y_0, \cdots, y_{m'-1}) \in X^{m+m'}$
を$x||y$と表記し、
$x \in (X^m)^N$，$y \in (X^{m'})^N$に対して、垂直結合
$(x_0||y_0, \cdots, x_{N-1}||y_{N-1})$
を$x||_V y$と表記し、
［ｘ］を値ｘを秘密分散で秘匿した値とし、
集合Ｘに対して［Ｘ］をＸの元を秘匿した値の集合とし、
ｍ、μをそれぞれ計算すべき出力関数Ｆの入力数、出力数とし、
レコード数をＮ、挿入するダミーレコード数を｜Ｄ｜、ランダム化系列数をν∈Ｅとし、
Πは秘密分散されたランダム置換データの集合を表すものとし、
前記ランダム化部が、
公開値から成るダミーレコード列$D \in (R^m)^{|D|}$を作成して出力するダミーレコード列作成部と、
前記ダミーレコード列Ｄを、正当性を持つ方法で秘匿し、秘匿済みダミーレコード列［Ｄ］$\in ([R]^m)^{|D|}$を取得するダミーレコード秘匿部と、
前記非ランダム化系列[Ａ]に前記秘匿されたダミーレコード列［Ｄ］を結合し、結合結果［Ａ||Ｄ］：＝［Ａ］||［Ｄ］を取得する結合部と、
$i < \nu$を充たすすべてのｉについて、前記結合結果［Ａ||Ｄ］に正当性をもつランダム置換処理を施して前記ランダム化系列$[B_i] := [\pi_i (A||D)]$を取得し、当該ランダム化系列と、利用された秘匿済みランダム置換データ$[\pi_i] \in [\Pi]$を出力するランダム置換部と、
をさらに含む秘密並列処理装置。
【請求項３】
請求項２に記載の秘密並列処理装置であって、
$0^{\rightarrow}$は空ベクトルを表すものとし、
前記計算部が、
前記非ランダム化系列、前記ランダム化系列、前記ダミーレコード列のチェックサムの初期値をそれぞれ$[C_A] := 0^{\rightarrow} \in ([R]^0)^N$，$[C_{B0}] := 0^{\rightarrow} \in ([R]^0)^{N+|D|}$，…，$[C_{B\nu-1}] := 0^{\rightarrow} \in ([R]^0)^{N+|D|}$，$[C_D] := 0^{\rightarrow} \in ([R]^0)^{|D|}$と定義するチェックサム初期値定義部と、
m_i，μ_iをそれぞれサブプロトコルf_iの入力数、出力数とし、
前記非ランダム化系列［Ａ］，前記ランダム化系列$[B_0]$，…，$[B_{\nu-1}]$のν＋１系列に対してｓｅｍｉ－ｈｏｎｅｓｔの秘密計算を施し、前記ダミーレコード列Ｄに対して平文の計算を施して、所望の関数Ｆを、サブプロトコル$f_i : [R]^{m_i} \rightarrow [R]^{\mu_i}$ごとに計算する関数計算部と、
前記サブプロトコル$f_i : [R]^{m_i} \rightarrow [R]^{\mu_i}$ごとにチェックサムを更新するチェックサム更新部と、
前記サブプロトコルf_iへのν＋２系列の各出力を、関数処理後非ランダム化系列$[A'] \in ([R]^{\mu_i})^N$，関数処理後ランダム化系列$[B'_0]$，…，$[B'_{\nu-1}] \in ([R]^{\mu_i})^{N+|D|}$，関数処理後ダミーレコード列$D' \in (R^{\mu_i})^{|D|}$と定義する関数処理後系列定義部と、
前記関数処理後ダミーレコード列Ｄ′を、正当性を持つ方法で秘匿し、秘匿済み関数処理後ダミーレコード列［Ｄ′］を取得する関数処理後ダミーレコード秘匿部と、
前記非ランダム化系列の出力チェックサム$[C_A] := [C_A]||_V [A']$と、$i < \nu$を充たすすべてのｉについての前記ランダム化系列の出力チェックサム$[C_{Bi}] := [C_{Bi}]||_V [B'_i]$と、前記ダミーレコード列の出力チェックサム$[C_D] := [$

C_D］||$_V$［D′］を出力する出力チェックサム生成部と、
をさらに含む秘密並列処理装置。
【請求項４】
請求項３に記載の秘密並列処理装置であって、
前記正当性証明部が、
受信すべき全データを受信したことを伝える信号であるデータ受信信号を、グループを構成する他の全秘密並列処理装置に送信し、前記グループを構成する他の全秘密並列処理装置からの当該信号を受信する第１データ受信信号送受信部と、
ｉ＜νを充たすすべてのｉについて、
前記秘匿済みランダム置換データ［π_i］を公開し、その復号値π_iを取得するランダム置換公開部と、
ｉ＜νを充たすすべてのｉについて、
Ｍを前記非ランダム化系列の出力チェックサム［C_A］、または前記ランダム化系列の出力チェックサム［C_{Bi}］の１レコード当たりの要素数とし、差分値［ζ_i］：＝［C_{Bi}］-（［C_A］||［C_D］）∈（［R］^{M}）$^{N+|D|}$を計算する差分値計算部と、
ｉ＜νを充たすすべてのｉについて、
前記差分値［ζ_i］の各レコードを、分割単位σ要素ごとに垂直分割し、差分分割値［ζ'_i］∈（［R］$^\sigma$）$^{(N+|D|)M'}$を取得する垂直分割部と、
ｉ＜νを充たすすべてのｉについて、
乱数の分散値［ρ_i］∈（［R］$^\sigma$）$^{(N+|D|)M'}$を生成する乱数分散値生成部と、
積和プロトコルにより積和値
【数２】

$$[\phi]=\sum_{i<\nu}[\rho_i][\zeta'_i]$$

を計算する積和部と、
受信すべき全データを受信したことを伝える信号であるデータ受信信号を、前記グループを構成する他の全秘密並列処理装置に送信し、前記グループを構成する他の全秘密並列処理装置からの当該信号を受信する第２データ受信信号送受信部と、
前記積和値［φ］を公開してその復号値φを取得する積和値公開部と、
前記積和値の復号値φ＝０を確認し、真ならば⊤、偽ならば⊥となる検証結果を前記グループを構成する他の全秘密並列処理装置に送信し、前記グループを構成する他の全秘密並列処理装置から前記検証結果を受信する検証結果送受信部と、
前記グループを構成する他の全秘密並列処理装置からの検証結果に⊥が存在すれば⊥、そうでなければ⊤となる最終検証結果を出力する最終検証結果出力部と、
をさらに含む秘密並列処理装置。
【請求項５】
秘密並列処理装置が実行する秘密並列処理方法であって、
前記秘密並列処理装置のランダム化部が、入力列である非ランダム化系列を取得して、前記非ランダム化系列と公開値からなるダミーレコード列とを結合してランダム置換処理したランダム化系列と、利用されたランダム置換データを秘匿した秘匿済みランダム置換データを出力するランダム化ステップを実行し、
前記秘密並列処理装置の計算部が、前記非ランダム化系列と、前記ランダム化系列と、前記ダミーレコード列を取得して、これらに所定の関数を施して、当該関数を施す処理における計算過程のデータを用いて各系列の出力チェックサムを生成する計算ステップを実行し、
前記秘密並列処理装置の正当性証明部が、前記各系列の出力チェックサムと、前記秘匿済みランダム置換データを取得して、前記各系列の出力チェックサムを評価して、前記非ランダム化系列に前記所定の関数が正しく施されたか否かの最終検証結果を出力する正当

性証明ステップを実行する
秘密並列処理方法。
【請求項６】
請求項５に記載の秘密並列処理方法であって、
平文空間をＲとし、
関数ｆ：Ｒ→Ｒ′に対して、$f^N : R^N \to R'^N$をｆの並列実行、すなわち
$f^N(a_0, \cdots, a_{N-1}) = (f(a_0), \cdots, f(a_{N-1}))$とし、
環Ｒに対して0_RをＲの零元とし、
Ｘを任意の集合とし、
ｍおよびｍ′を任意の整数とし、
ｉを任意の整数とし、
X^mの元ｘに対して、ｉ番目の要素をx_iと表記し、
$x \in X^m$，$y \in X^{m'}$に対して、結合
$(x_0, \cdots, x_{m-1}, y_0, \cdots, y_{m'-1}) \in X^{m+m'}$
をｘ||ｙと表記し、
$x \in (X^m)^N$，$y \in (X^{m'})^N$に対して、垂直結合
$(x_0 || y_0, \cdots, x_{N-1} || y_{N-1})$
を$x ||_V y$と表記し、
［ｘ］を値ｘを秘密分散で秘匿した値とし、
集合Ｘに対して［Ｘ］をＸの元を秘匿した値の集合とし、
ｍ、μをそれぞれ計算すべき出力関数Ｆの入力数、出力数とし、
レコード数をＮ、挿入するダミーレコード数を｜Ｄ｜、ランダム化系列数を$\nu \in E$とし、
Πは秘密分散されたランダム置換データの集合を表すものとし、
前記ランダム化ステップが、
公開値から成るダミーレコード列$D \in (R^m)^{|D|}$を作成して出力するダミーレコード列作成ステップと、
前記ダミーレコード列Ｄを、正当性を持つ方法で秘匿し、秘匿済みダミーレコード列［Ｄ］$\in ([R]^m)^{|D|}$を取得するダミーレコード秘匿ステップと、
前記非ランダム化系列[Ａ]に前記秘匿されたダミーレコード列［Ｄ］を結合し、結合結果［Ａ||Ｄ］：＝［Ａ］||［Ｄ］を取得する結合ステップと、
$i < \nu$を充たすすべてのｉについて、前記結合結果［Ａ||Ｄ］に正当性をもつランダム置換処理を施して前記ランダム化系列$[B_i] := [\pi_i(A||D)]$を取得し、当該ランダム化系列と、利用された秘匿済みランダム置換データ$[\pi_i] \in [\Pi]$を出力するランダム置換ステップと、
をさらに含む秘密並列処理方法。
【請求項７】
請求項６に記載の秘密並列処理方法であって、　$0^{\rightarrow}$は空ベクトルを表すものとし、
前記計算ステップが、
前記非ランダム化系列、前記ランダム化系列、前記ダミーレコード列のチェックサムの初期値をそれぞれ$[C_A] := 0^{\rightarrow} \in ([R]^0)^N$，$[C_{B_0}] := 0^{\rightarrow} \in ([R]^0)^{N+|D|}$，…，$[C_{B_{\nu-1}}] := 0^{\rightarrow} \in ([R]^0)^{N+|D|}$，$[C_D] := 0^{\rightarrow} \in ([R]^0)^{|D|}$と定義するチェックサム初期値定義ステップと、
m_i，μ_iをそれぞれサブプロトコルf_iの入力数、出力数とし、
前記非ランダム化系列［Ａ］，前記ランダム化系列$[B_0]$，…，$[B_{\nu-1}]$のν＋１系列に対してｓｅｍｉ－ｈｏｎｅｓｔの秘密計算を施し、前記ダミーレコード列Ｄに対して平文の計算を施して、所望の関数Ｆを、サブプロトコル$f_i : [R]^{m_i} \to [R]^{\mu_i}$ごとに計算する関数計算ステップと、
前記サブプロトコル$f_i : [R]^{m_i} \to [R]^{\mu_i}$ごとにチェックサムを更新するチェックサム更新ステップと、

前記サブプロトコルf_iへのν＋２系列の各出力を、関数処理後非ランダム化系列［A′］∈（［R］$^{\mu i}$）^{N}，関数処理後ランダム化系列［B′$_0$］，…，［B′$_{\nu-1}$］∈（［R］$^{\mu i}$）$^{N+|D|}$，関数処理後ダミーレコード列D′∈（R$^{\mu i}$）$^{|D|}$と定義する関数処理後系列定義ステップと、

前記関数処理後ダミーレコード列D′を、正当性を持つ方法で秘匿し、秘匿済み関数処理後ダミーレコード列［D′］を取得する関数処理後ダミーレコード秘匿ステップと、

前記非ランダム化系列の出力チェックサム［C_A］：＝［C_A］||$_V$［A′］と、i＜νを充たすすべてのiについての前記ランダム化系列の出力チェックサム［C_{Bi}］：＝［C_{Bi}］||$_V$［B′$_i$］と、前記ダミーレコード列の出力チェックサム［C_D］：＝［C_D］||$_V$［D′］を出力する出力チェックサム生成ステップと、

をさらに含む秘密並列処理方法。

【請求項８】

請求項７に記載の秘密並列処理方法であって、

前記正当性証明ステップが、

受信すべき全データを受信したことを伝える信号であるデータ受信信号を、グループを構成する他の全秘密並列処理装置に送信し、前記グループを構成する他の全秘密並列処理装置からの当該信号を受信する第１データ受信信号送受信ステップと、

i＜νを充たすすべてのiについて、

前記秘匿済みランダム置換データ［π_i］を公開し、その復号値π_iを取得するランダム置換公開ステップと、

i＜νを充たすすべてのiについて、

Mを前記非ランダム化系列の出力チェックサム［C_A］、または前記ランダム化系列の出力チェックサム［C_{Bi}］の１レコード当たりの要素数とし、差分値［ζ_i］：＝［C_{Bi}］-（［C_A］||［C_D］）∈（［R］^{M}）$^{N+|D|}$を計算する差分値計算ステップと、

i＜νを充たすすべてのiについて、

前記差分値［ζ_i］の各レコードを、分割単位σ要素ごとに垂直分割し、差分分割値［ζ'_i］∈（［R］$^{\sigma}$）$^{(N+|D|)M'}$を取得する垂直分割ステップと、

i＜νを充たすすべてのiについて、

乱数の分散値［ρ_i］∈（［R］$^{\sigma}$）$^{(N+|D|)M'}$を生成する乱数分散値生成ステップと、

積和プロトコルにより積和値

【数３】

$$[\phi]=\sum_{i<\nu}[\rho_i][\zeta'_i]$$

を計算する積和ステップと、

受信すべき全データを受信したことを伝える信号であるデータ受信信号を、前記グループを構成する他の全秘密並列処理装置に送信し、前記グループを構成する他の全秘密並列処理装置からの当該信号を受信する第２データ受信信号送受信ステップと、

前記積和値［φ］を公開してその復号値φを取得する積和値公開ステップと、

前記積和値の復号値φ＝０を確認し、真ならば⊤、偽ならば⊥となる検証結果を前記グループを構成する他の全秘密並列処理装置に送信し、前記グループを構成する他の全秘密並列処理装置から前記検証結果を受信する検証結果送受信ステップと、

前記グループを構成する他の全秘密並列処理装置からの検証結果に⊥が存在すれば⊥、そうでなければ⊤となる最終検証結果を出力する最終検証結果出力ステップと、

をさらに含む秘密並列処理方法。

【請求項９】

コンピュータを、請求項１から４のいずれかに記載の秘密並列処理装置として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】
本発明は計算結果の正当性を保ちながら秘密分散によりデータを秘匿しつつデータ処理を行う秘密並列処理装置、秘密並列処理方法、プログラムに関する。
【背景技術】
【０００２】
従来の正当性を保つ秘密計算方法として、例えば非特許文献１がある。
【先行技術文献】
【非特許文献】
【０００３】
【非特許文献１】五十嵐大、濱田浩気、菊池亮、千田浩司、「非常に高効率なｎ＞＝２ｋ－１のｍａｌｉｃｉｏｕｓモデル上秘密分散ベース秘密計算」、ＳＣＩＳ２０１３（暗号と情報セキュリティシンポジウム）暗号プロトコルセッション（３Ｃ３－２）
【発明の概要】
【発明が解決しようとする課題】
【０００４】
上記の従来技術においては、セキュリティパラメータκ（すなわち改ざん成功率が１／2^{κ}程度）、処理の規模を表すパラメータＣにおける通信量がＯ（κＣ）ビットとなり通信コストが大きいという課題があった。そこで本発明では、秘密並列処理において通信量を削減することができる秘密並列処理装置を提供することを目的とする。
【課題を解決するための手段】
【０００５】
本発明の秘密並列処理装置は、ランダム化部と、計算部と、正当性証明部を含む。
【０００６】
ランダム化部は、入力列である非ランダム化系列を取得して、非ランダム化系列と公開値からなるダミーレコード列とを結合してランダム置換処理したランダム化系列と、利用されたランダム置換データを秘匿した秘匿済みランダム置換データを出力する。計算部は、非ランダム化系列と、ランダム化系列と、ダミーレコード列を取得して、これらに所定の関数を施して、当該関数を施す処理における計算過程のデータを用いて各系列の出力チェックサムを生成する。正当性証明部は、各系列の出力チェックサムと、秘匿済みランダム置換データを取得して、各系列の出力チェックサムを評価して、非ランダム化系列に所定の関数が正しく施されたか否かの最終検証結果を出力する。
【発明の効果】
【０００７】
本発明の秘密並列処理装置によれば、秘密並列処理において通信量を削減することができる。
【図面の簡単な説明】
【０００８】
【図１】実施例１の秘密並列処理装置の構成を示すブロック図。
【図２】実施例１の秘密並列処理装置の動作を示すフローチャート。
【図３】実施例１の秘密並列処理装置のランダム化部の構成を示すブロック図。
【図４】実施例１の秘密並列処理装置のランダム化部の動作を示すフローチャート。
【図５】実施例１の秘密並列処理装置の計算部の構成を示すブロック図。
【図６】実施例１の秘密並列処理装置の計算部の動作を示すフローチャート。
【図７】実施例１の秘密並列処理装置の正当性証明部の構成を示すブロック図。
【図８】実施例１の秘密並列処理装置の正当性証明部の動作を示すフローチャート。
【発明を実施するための形態】
【０００９】
以下、本発明の実施の形態について、詳細に説明する。なお、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。

【実施例１】

【００１０】

＜記法＞

以下、本明細書において共通で使用される記法について説明する。

平文空間をＲとする。

関数ｆ：Ｒ→Ｒ′に対して、$f^N : R^N \to R'^N$をｆの並列実行、すなわち
$f^N(a_0, \cdots, a_{N-1}) = (f(a_0), \cdots, f(a_{N-1}))$とする。

環Ｒに対して0_RをＲの零元とする。

Ｘを任意の集合とし、ｍおよびｍ′を任意の整数とする。X^mの元ｘに対して、ｉを任意の整数とし、ｉ番目の要素をx_iと表記する。

$x \in X^m$，$y \in X^{m'}$に対して、結合
$(x_0, \cdots, x_{m-1}, y_0, \cdots, y_{m'-1}) \in X^{m+m'}$
をｘ||ｙと表記する。

$x \in (X^m)^N$，$y \in (X^{m'})^N$に対して、垂直結合
$(x_0||y_0, \cdots, x_{N-1}||y_{N-1})$
を$x||_V y$と表記する。

［ｘ］は値ｘを秘密分散で秘匿した値、また集合Ｘに対して、［Ｘ］はＸの元を秘匿した値の集合とする。

【００１１】

＜秘密並列処理装置の概要＞

以下、図１を参照して、本実施例の秘密並列処理装置の概要について説明する。図１は、本実施例の秘密並列処理装置１の構成を示すブロック図である。図１に示すように、本実施例の秘密並列処理装置１は、ランダム化部１１と、計算部１２と、正当性証明部１３を含む構成である。ランダム化部１１、計算部１２には、入力列（非ランダム化系列と呼ぶ）が入力される。正当性証明部１３は、最終検証結果を出力する。秘密並列処理装置１は、複数台でグループを構成し、グループで以下の処理を実行することにより、秘密並列処理を実現する。

【００１２】

＜秘密並列処理方法の概要＞

以下、図２を参照して、本実施例の秘密並列処理方法の概要について説明する。図２は、本実施例の秘密並列処理装置１の動作を示すフローチャートである。図２に示すように、本実施例の秘密並列処理方法は、ランダム化ステップ（ステップＳ１１、スキーム１）、計算ステップ（ステップＳ１２、スキーム２）、正当性証明ステップ（ステップＳ１３、スキーム３）の３ステップに分かれて順に行われる。ランダム化部１１は、ランダム化ステップを実行し、計算部１２は、計算ステップを実行し、正当性証明部１３は、正当性証明ステップを実行するものとする。

【００１３】

ランダム化部１１は、入力列である非ランダム化系列を取得して、非ランダム化系列と公開値からなるダミーレコード列とを結合してランダム置換処理したランダム化系列と、利用されたランダム置換データを秘匿した秘匿済みランダム置換データを出力する（Ｓ１１）。なお、公開値とは、グループ内の全装置に公開されている値のことである。また、置換データとは、例えば各要素が０からＮ－１の異なる数であるようなＮ要素の列であって、Ｎ要素のデータの置換の仕方を表す。例示すれば、（ａ＿０，ａ＿１，ａ＿２）のＮ＝３のデータに対して置換データ（２，１，０）で置換するとは、ａ＿０を２番目に、ａ＿１を１番目に、ａ＿２を０番目に移動して（ａ＿２，ａ＿１，ａ＿０）とする。乱数により生成されたランダムな置換データを、ランダム置換データと呼ぶ。秘匿されたランダム置換データとは例えば、参考非特許文献２の方法では、グループ内のｋ装置の組（グループの装置数ｎとすると、$_nC_k$種類存在する）がそれぞれ、計$_nC_k$個のランダム置換データを共有した、そのランダム置換データの集合であり、置換を実行する際にはこれら

の全ての置換データを用いて順に置換を行う。このような秘匿されたランダム置換データでは、どのｎ－ｋ装置の組を見ても、少なくとも１つ共有されていないランダム置換データが存在するため、全体の置換は秘匿される。

【００１４】

計算部１２は、非ランダム化系列と、ランダム化系列と、ダミーレコード列を取得して、これらに所定の関数を施して、当該関数を施す処理における計算過程のデータを用いて各系列の出力チェックサムを生成する（Ｓ１２）。正当性証明部１３は、各系列の出力チェックサムと、秘匿済みランダム置換データを取得して、各系列の出力チェックサムを評価して、非ランダム化系列に所定の関数が正しく施されたか否かの最終検証結果を出力する（Ｓ１３）。

【００１５】

＜ランダム化部１１＞

以下、図３、図４を参照してランダム化部１１、およびランダム化部１１が実行するランダム化ステップ（Ｓ１１、スキーム１）の詳細について説明する。図３は本実施例の秘密並列処理装置１のランダム化部１１の構成を示すブロック図である。図４は本実施例の秘密並列処理装置１のランダム化部１１の動作を示すフローチャートである。図３に示すように、ランダム化部１１は、ダミーレコード列作成部１１１と、ダミーレコード秘匿部１１２と、結合部１１３と、ランダム置換部１１４を含む。

【００１６】

スキーム１では、ダミーレコード列を追加して、正当性を持つランダム置換処理をν回行う。パラメータνは、ν＝┌κ／ｌｏｇＮ┐程度の整数である。なお公開値の分散は、秘密並列処理を実行するグループ内の各装置が乱数成分固定として自分のシェアを作成すればよく、オフライン処理である。なお正当性をもつランダム置換処理は任意である。例えば参考非特許文献１に記載の正当性を持つランダム置換処理や、または参考非特許文献１の正当性を持たないランダム置換処理や、参考非特許文献２のランダム置換処理に前述の非特許文献１の変換方法を組み合わせたランダム置換処理などがある。

（参考非特許文献１）S. Laur, J. Willemson, and B. Zhang. Round-efficient oblivious database manipulation.In X. Lai, J. Zhou, and H. Li eds., ISC, Vol. 7001 of Lecture Notes in Computer Science, pp. 262-277. Springer, 2011.

（参考非特許文献２）濱田浩気、五十嵐大、千田浩司、高橋克巳、「３パーティ秘匿関数計算のランダム置換プロトコル」、情報処理学会シンポジウム論文集、2010年10月12日、2010巻、第9号、pp561-566

【００１７】

また公開値ｘを正当性を持って秘密分散によりあるｎ個に秘匿するのはグループ内の各装置が以下の処理を行えばよい。いかなる秘密分散にも適用可能である。

１）秘密分散では通常乱数を生成するが、この乱数を全て０などの定数とする。

２）入力をｘ、乱数を上記の定数として秘密分散アルゴリズムによりｎ個のシェアを得る。

３）ｎ個のうち自分の持ち分のシェアのみを出力する。

【００１８】

ｘは公開値であるので上記は通信無しでグループ内の各装置のみで実行することができる。通信無しの処理が秘密計算として正当性を持つことはよく知られており、よって上記の秘匿は正当性を持つ。

【００１９】

スキーム１で使用されるパラメータ、入力、出力を以下に示す。

パラメータ：計算すべきｍ入力μ出力関数Ｆ（ｍ、μをそれぞれ計算すべき出力関数Ｆの入力数、出力数とする）、レコード数Ｎ、挿入するダミーレコード数｜Ｄ｜、ランダム化系列数ν∈Ｅ（Ｅは任意の自然数の集合）

入力：非ランダム化系列［Ａ］∈（［Ｒ］^{m}）^{N}

出力：秘匿済みランダム置換データ［π_0］，…，［$\pi_{\nu-1}$］∈［$\Pi^{N+|D|}$］ラン

ダム化系列［B_0］＝［π_0（A||D）］，…，［$B_{\nu-1}$］＝［$\pi_{\nu-1}$（A||D）］∈（［R］$^{\mu}$）$^{N+|D|}$，ダミーレコード列D∈（R^m）$^{|D|}$、ただし、Πは秘匿済みランダム置換データの集合を表す。

【００２０】

＜ステップＳ１１１＞

ダミーレコード列作成部１１１は、公開値から成るダミーレコード列D∈（R^m）$^{|D|}$を作成して出力する（Ｓ１１１）。内容は$F^{|D|}$の定義域内で任意である。

【００２１】

＜ステップＳ１１２＞

ダミーレコード秘匿部１１２は、ダミーレコード列Dを、正当性を持つ方法で秘匿し、秘匿済みダミーレコード列［D］∈（［R］^{m}）$^{|D|}$を取得する（Ｓ１１２）。

【００２２】

＜ステップＳ１１３＞

結合部１１３は、入力（非ランダム化系列［A］）に秘匿されたダミーレコード列［D］を結合し、結合結果［A||D］：＝［A］||［D］を取得する（Ｓ１１３）。

【００２３】

以下のステップＳ１１４は、ｉ＜νを充たすすべてのｉについて実行される。

＜ステップＳ１１４＞

ランダム置換部１１４は、結合結果［A||D］に正当性をもつランダム置換処理を施してランダム化系列［B_i］：＝［π_i（A||D）］を取得し、当該ランダム化系列と、利用された秘匿済みランダム置換データ［π_i］∈［Π］を出力する（Ｓ１１４）。

【００２４】

＜計算部１２＞

以下、図５、図６を参照して計算部１２、および計算部１２が実行する計算ステップ（Ｓ１２、スキーム２）の詳細について説明する。図５は本実施例の秘密並列処理装置１の計算部１２の構成を示すブロック図である。図６は本実施例の秘密並列処理装置１の計算部１２の動作を示すフローチャートである。図５に示すように、計算部１２は、チェックサム初期値定義部１２１と、関数計算部１２２と、チェックサム更新部１２３と、関数処理後系列定義部１２４と、関数処理後ダミーレコード秘匿部１２５と、出力チェックサム生成部１２６を含む。

【００２５】

スキーム２では、非ランダム化系列、ランダム化系列、ダミーレコード列の３系列で所望の関数Ｆを並列に計算する。その際、出力は全てチェックサムとして保存される。

【００２６】

スキーム２で使用されるパラメータ、入力、出力を以下に示す。

パラメータ：計算すべきm入力μ出力関数Ｆ、レコード数Ｎ、挿入するダミーレコード数｜Ｄ｜，ランダム化系列数ν∈Ｅ（Ｅは任意の自然数の集合）

入力：非ランダム化系列［A］∈（［R］^{m}）^{N}，ランダム化系列［B_0］，…，［$B_{\nu-1}$］∈（［R］$^{\mu}$）$^{N+|D|}$，ダミーレコード列D∈（R^m）$^{|D|}$

出力：出力［F^N（A）］∈（［R］$^{\mu}$）^{N}，ν＋２個のチェックサム［C_A］，［C_{B_0}］，…，［$C_{B_{\nu-1}}$］，［C_D］

【００２７】

＜ステップＳ１２１＞

チェックサム初期値定義部１２１は、非ランダム化系列、ランダム化系列、ダミーレコード列のチェックサムの初期値をそれぞれ［C_A］：＝$0^{\rightarrow}$∈（［R］^{0}）^{N}，［C_{B_0}］：＝$0^{\rightarrow}$∈（［R］^{0}）$^{N+|D|}$，…，［$C_{B_{\nu-1}}$］：＝$0^{\rightarrow}$∈（［R］^{0}）$^{N+|D|}$，［C_D］：＝$0^{\rightarrow}$∈（［R］^{0}）$^{|D|}$と定義する（Ｓ１２１）。ただし$0^{\rightarrow}$は空ベクトルである。

【００２８】

＜ステップＳ１２２＞

関数計算部１２２は、非ランダム化系列［Ａ］，ランダム化系列［B_0］，…，［$B_{\nu-1}$］のν＋１系列に対してｓｅｍｉ－ｈｏｎｅｓｔの秘密計算を施し、ダミーレコード列Ｄに対して平文の計算を施して、所望の関数Ｆを、サブプロトコルf_i：［Ｒ］^{m_i}→［Ｒ］$^{\mu_i}$ごとに計算し、［F^N（Ａ）］∈（［Ｒ］$^{\mu}$）^{N}を出力する（Ｓ１２２）。ただしm_i，μ_iはそれぞれサブプロトコルf_iの入力数、出力数である。

【００２９】

＜ステップＳ１２３＞

チェックサム更新部１２３は、前述したサブプロトコルf_i：［Ｒ］^{m_i}→［Ｒ］$^{\mu_i}$ごとにチェックサムを更新する（Ｓ１２３）。

【００３０】

＜ステップＳ１２４＞

関数処理後系列定義部１２４は、サブプロトコルf_iへのν＋２系列の各出力を、関数処理後非ランダム化系列［Ａ′］∈（［Ｒ］$^{\mu_i}$）^{N}，関数処理後ランダム化系列［B'_0］，…，［$B'_{\nu-1}$］∈（［Ｒ］$^{\mu_i}$）$^{N+|D|}$，関数処理後ダミーレコード列Ｄ′∈（R^{μ_i}）$^{|D|}$と定義する（Ｓ１２４）。

【００３１】

＜ステップＳ１２５＞

関数処理後ダミーレコード秘匿部１２５は、関数処理後ダミーレコード列Ｄ′を、正当性を持つ方法で秘匿し、秘匿済み関数処理後ダミーレコード列［Ｄ′］を取得する（Ｓ１２５）。

【００３２】

＜ステップＳ１２６＞

出力チェックサム生成部１２６は、非ランダム化系列のチェックサム［C_A］と関数処理後非ランダム化系列［Ａ′］を垂直結合して非ランダム化系列の出力チェックサム（［C_A］：＝［C_A］$||_V$［Ａ′］）を生成して出力する（Ｓ１２６）。出力チェックサム生成部１２６は、ｉ＜νを充たすすべてのｉについてランダム化系列のチェックサム［C_{B_i}］と関数処理後ランダム化系列［B'_i］を垂直結合してランダム化系列の出力チェックサム（［C_{B_i}］：＝［C_{B_i}］$||_V$［B'_i］）を生成して出力する（Ｓ１２６）。出力チェックサム生成部１２６は、ダミーレコード列のチェックサム［C_D］と秘匿済み関数処理後ダミーレコード列［Ｄ′］を垂直結合してダミーレコード列の出力チェックサム（［C_D］：＝［C_D］$||_V$［Ｄ′］）を生成して出力する（Ｓ１２６）。

【００３３】

＜正当性証明部１３＞

以下、図７、図８を参照して正当性証明部１３、および正当性証明部１３が実行する正当性証明ステップ（Ｓ１３、スキーム３）の詳細について説明する。図７は本実施例の秘密並列処理装置１の正当性証明部１３の構成を示すブロック図である。図８は本実施例の秘密並列処理装置１の正当性証明部１３の動作を示すフローチャートである。図７に示すように、正当性証明部１３は、第１データ受信信号送受信部１３０と、ランダム置換公開部１３１と、差分値計算部１３２と、垂直分割部１３３と、乱数分散値生成部１３４と、積和部１３５と、第２データ受信信号送受信部１３６と、積和値公開部１３７と、検証結果送受信部１３８と、最終検証結果出力部１３９を含む。

【００３４】

スキーム３では計算ステップで保存されたチェックサムを元に正当性を検証する。記号ＳＹＮＣは、その時点までの全ての受信すべきデータを受信したことをグループ内の他の全装置に伝える信号を送信し、またグループ内の他の全装置からの当該信号を受信する処理を示す。ＳＹＮＣが確認できるまでは後続の処理を行わないことで非同期ネットワークでのセキュリティを担保する。

【００３５】

スキーム３で使用されるパラメータ、入力、出力を以下に示す。

パラメータ：計算すべきｍ入力μ出力関数Ｆ，レコード数Ｎ，挿入するダミーレコード数

｜Ｄ｜，ランダム化系列数ν∈Ｅ（Ｅは任意の自然数の集合），分割単位σ∈Ｅ
入力：出力チェックサム［C_A］，［C_{B0}］，…，［$C_{B\nu-1}$］，［C_D］，秘匿済みランダム置換データ［π_0］，…，［$\pi_{\nu-1}$］∈［$\Pi^{N+|D|}$］
出力：改ざんがあれば改ざんがあったことを示す最終検証結果┴、改ざんがなければ改ざんがなかったことを示す最終検証結果┬
【００３６】
＜ステップＳ１３０＞
第１データ受信信号送受信部１３０は、前述のＳＹＮＣ処理を実行する（Ｓ１３０）。具体的には、第１データ受信信号送受信部１３０は、ステップＳ１３０までに受信すべき全データを受信したことを伝える信号であるデータ受信信号をグループ内の他の全装置に送信し、またグループ内の他の全装置からの当該信号を受信する（Ｓ１３０）。
【００３７】
以下のステップＳ１３１からステップＳ１３５は、ｉ＜νを充たすすべてのｉについて実行される。
＜ステップＳ１３１＞
ランダム置換公開部１３１は、秘匿済みランダム置換データ［π_i］を公開し、その復号値π_iを取得する（Ｓ１３１）。
【００３８】
＜ステップＳ１３２＞
差分値計算部１３２は、ランダム化系列の出力チェックサム［C_{Bi}］から非ランダム化系列の出力チェックサム［C_A］とダミーレコード列の出力チェックサム［C_D］の結合（［C_A］||［C_D］）を差し引いた差分値［ζ_i］を計算する（Ｓ１３２）。すなわち、差分値計算部１３２は、差分値［ζ_i］：＝［C_{Bi}］-（［C_A］||［C_D］）∈（［Ｒ］^{M}）$^{N+|D|}$を計算する（Ｓ１３２）。なおＭは［C_A］（または［C_{Bi}］、どちらでも等しい）の１レコード当たりの要素数とする。
【００３９】
＜ステップＳ１３３＞
垂直分割部１３３は、差分値［ζ_i］の各レコードを、分割単位σ要素ごとに垂直分割する（Ｓ１３３）。垂直分割部１３３は、（［Ｒ］$^\sigma$）$^{N+|D|}$の要素をＭ′＝┌Ｍ／σ┐個取得する。なお最後の分割に端数が現れる場合、垂直分割部１３３は、σ要素に満たない部分を０パディングする。垂直分割部１３３は、差分分割値［ζ'_i］∈（［Ｒ］$^\sigma$）$^{(N+|D|)M'}$を取得する（Ｓ１３３）。
【００４０】
＜ステップＳ１３４＞
乱数分散値生成部１３４は、乱数の分散値［ρ_i］∈（［Ｒ］$^\sigma$）$^{(N+|D|)M'}$を生成する（Ｓ１３４）。
【００４１】
＜ステップＳ１３５＞
積和部１３５は、差分分割値と乱数の分散値に基づいて、積和プロトコルにより積和値
【数１】

$$[\phi]=\sum_{i<\nu}[\rho_i][\zeta'_i]$$

を計算する（Ｓ１３５）。
【００４２】
＜ステップＳ１３６＞
第２データ受信信号送受信部１３６は、ＳＹＮＣ処理を実行する（Ｓ１３６）。具体的には、第２データ受信信号送受信部１３６は、ステップＳ１３６までに受信すべき全データを受信したことを伝える信号であるデータ受信信号をグループ内の他の全装置に送信し、またグループ内の他の全装置からの当該信号を受信する（Ｓ１３６）。

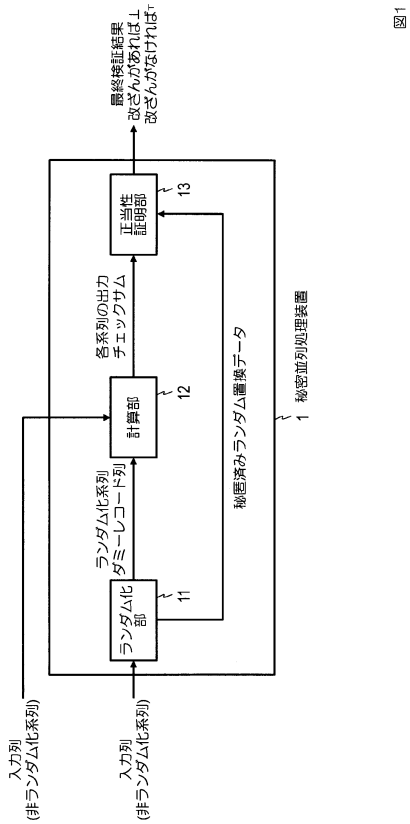
【００４３】
＜ステップＳ１３７＞
積和値公開部１３７は、積和値［φ］を公開してその復号値φを取得する（Ｓ１３７）。
【００４４】
＜ステップＳ１３８＞
検証結果送受信部１３８は、積和値の復号値φ＝０を確認し、真ならば⊤、偽ならば⊥となる検証結果をグループ内の他の全装置に送信し、グループ内の他の全装置から検証結果を受信する（Ｓ１３８）。
【００４５】
＜ステップＳ１３９＞
最終検証結果出力部１３９は、グループ内の他の全装置からの検証結果に⊥が存在すれば⊥、そうでなければ⊤となる最終検証結果を出力する（Ｓ１３９）。
本実施例の秘密並列処理装置１によれば、秘密並列処理において通信量を削減することができる。具体的には、データ並列数Ｎの計算を行う際に通信量Ｏ（┌κ／ｌｏｇＮ┐Ｃ）ビットとすることができ、通信量に関し、従来法よりもｌｏｇＮ改善される。
【００４６】
＜本発明のポイント＞
従来処理結果の正当性を保証するためには代数的構造である体の性質が用いられてきた。しかしこの方針ではセキュリティパラメータκはおよそ体のビット長と同程度となる。本発明ではランダム置換処理を用いてデータ並列数Ｎをセキュリティ強度に組み込むことができた。ダミーレコードは、中身は何でもよいにも関わらず、ダミーレコード無しではセキュリティが達成されない点もポイントである。
【００４７】
上述の各種の処理は、記載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。その他、本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。
【００４８】
また、上述の構成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、上記処理機能がコンピュータ上で実現される。
【００４９】
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。
【００５０】
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。
【００５１】
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。

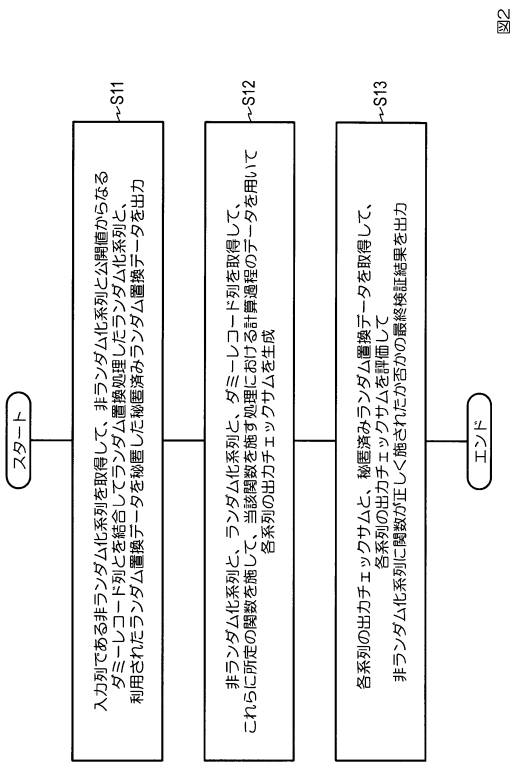
【００５２】

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。

【図１】



【図２】



【図３】

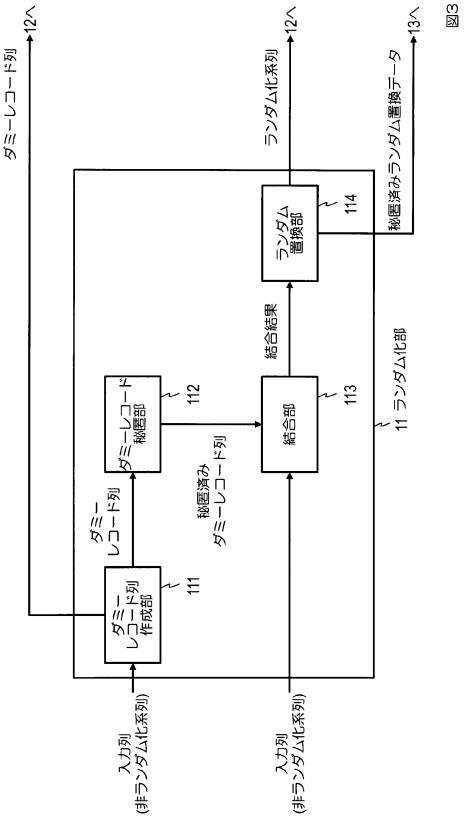


図3

【図４】

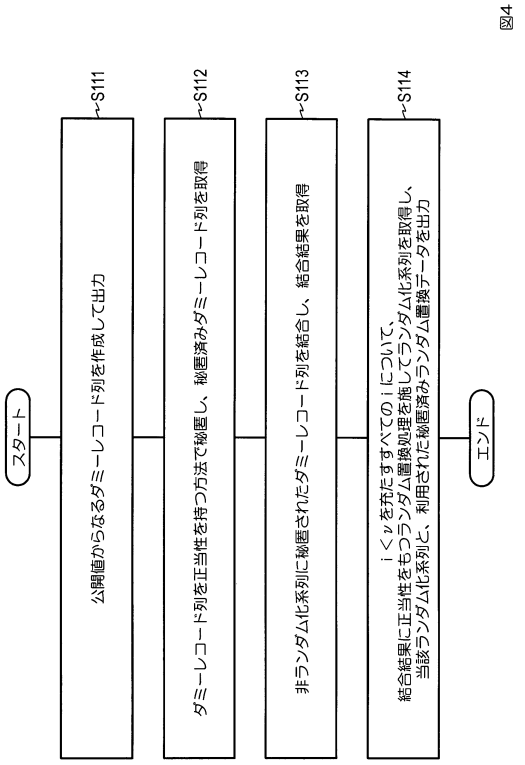


図4

【図５】

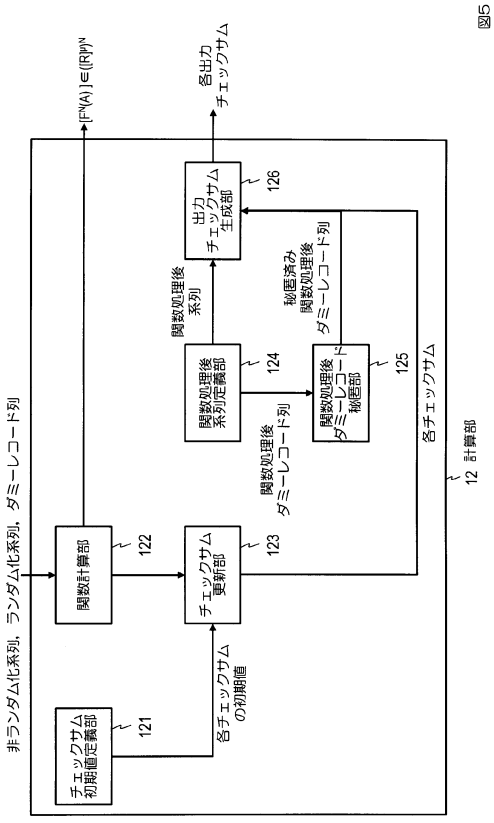


図5

【図６】

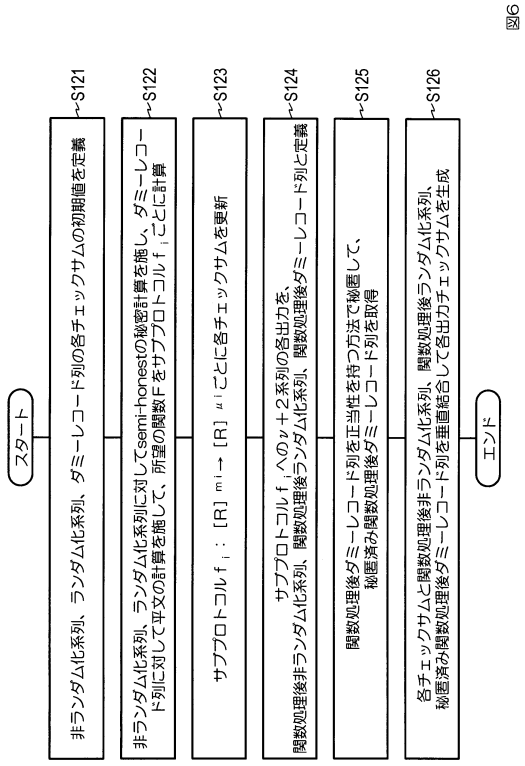


図6

【図７】

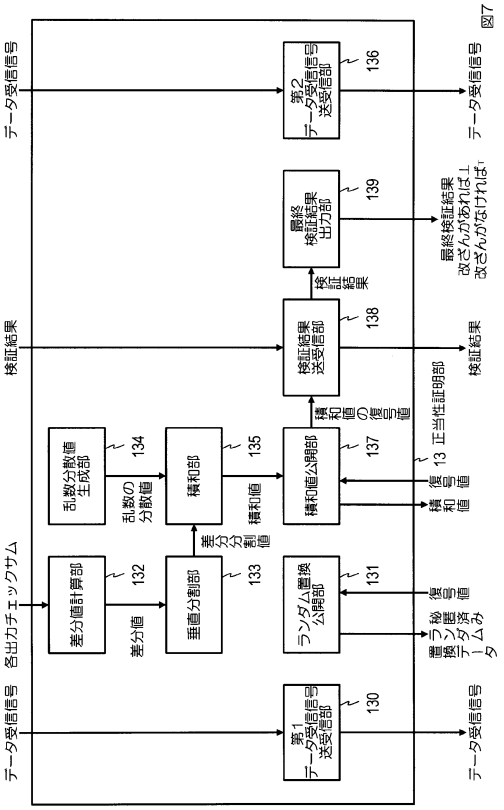

データ受信信号
各出力チェックサム
検証結果
データ受信信号
差分値計算部
132
差分値
垂直分割部
133
差分割値
ランダム置換公開部
131
秘匿ランダム置換データ
復号値
乱数分散値生成部
134
乱数の分散値
積和部
135
積和値
積和値公開部
137
積和値の復号値
正当性証明部
13
検証結果送受信部
138
検証結果
最終検証結果出力部
139
最終検証結果
改ざんがあれば⊥
改ざんがなければ「
第1データ受信信号送受信部
130
第2データ受信信号送受信部
136
データ受信信号
データ受信信号
検証結果
積和値の復号値

図7

【図８】

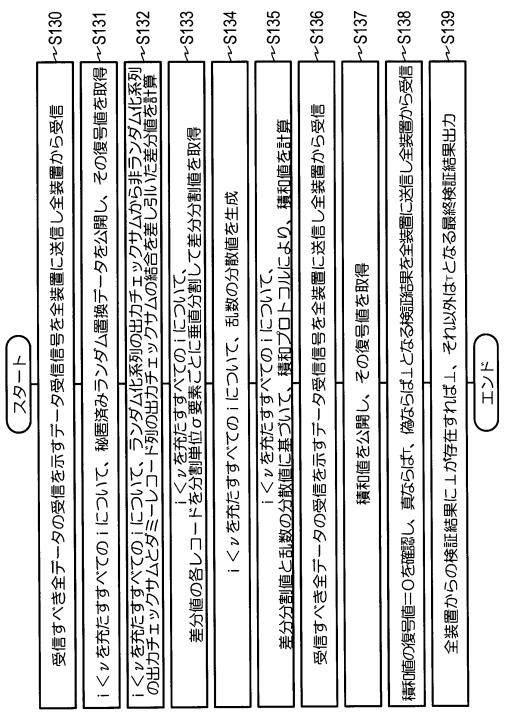

スタート
受信すべき全データの受信を示すデータ受信信号を全装置に送信し全装置から受信
~S130
i < ν を充たすすべての i について、秘匿済みランダム置換データを公開し、その復号値を取得
~S131
i < ν を充たすすべての i について、ランダム化系列の出力チェックサムから非ランダム化系列の出力チェックサムの結合を差し引いた差分値を計算
~S132
i < ν を充たすすべての i について、差分値の各レコードを分割単位の要素ごとに垂直分割して差分分割値を取得
~S133
i < ν を充たすすべての i について、乱数の分散値を生成
~S134
i < ν を充たすすべての i について、差分分割値と乱数の分散値に基づいて、積和プロトコルにより、積和値を計算
~S135
受信すべき全データの受信を示すデータ受信信号を全装置に送信し全装置から受信
~S136
積和値を公開し、その復号値を取得
~S137
積和値の復号値＝0を確認し、真ならば⊥となる検証結果を全装置に送信し全装置から受信
~S138
全装置からの検証結果に⊥が存在すれば⊥、それ以外は「となる最終検証結果出力
~S139
エンド

図8

フロントページの続き

(72)発明者　濱田　浩気
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
(72)発明者　千田　浩司
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　中里　裕正

(56)参考文献　国際公開第２００５／０７１６４０（WO，Ａ１）
米国特許第０６７７２３３９（ＵＳ，Ｂ１）
五十嵐大 他，２０１３年 暗号と情報セキュリティシンポジウム講演論文集，２０１３年　１月２２日，p.1-8

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／３２
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ　Ｘｐｌｏｒｅ