(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6713585号
(P6713585)
(45)発行日　令和2年6月24日(2020.6.24)　(24)登録日　令和2年6月5日(2020.6.5)

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

請求項の数 9　(全 15 頁)

(21)出願番号　特願2019-527663(P2019-527663)
(86)(22)出願日　平成30年6月28日(2018.6.28)
(86)国際出願番号　PCT/JP2018/024588
(87)国際公開番号　WO2019/009180
(87)国際公開日　平成31年1月10日(2019.1.10)
審査請求日　令和1年12月5日(2019.12.5)
(31)優先権主張番号　特願2017-132034(P2017-132034)
(32)優先日　平成29年7月5日(2017.7.5)
(33)優先権主張国・地域又は機関
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　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

最終頁に続く

(54)【発明の名称】秘密計算システム、秘密計算装置、秘密計算方法、プログラム、および記録媒体

(57)【特許請求の範囲】
【請求項１】
秘密計算装置P_0と秘密計算装置P_1と秘密計算装置P_2とを有し、
$i \in \{0, 1, 2\}$であり、P_+が$P_{(i+1) \bmod 3}$であり、P_-が$P_{(i-1) \bmod 3}$であり、a，bが任意値であり、a_0，a_1，a_2が$a = a_0 + a_1 + a_2$を満たすサブシェアであり、b_0，b_1，b_2が$b = b_0 + b_1 + b_2$を満たすサブシェアであり、
前記秘密計算装置P_iの記憶部と前記秘密計算装置P_+の記憶部とが前記サブシェア$a_+ \in \{a_0, a_1, a_2\}$および$b_+ \in \{b_0, b_1, b_2\}$を格納しており、
前記秘密計算装置P_iの記憶部と前記秘密計算装置P_-の記憶部とが前記サブシェア$a_- \in A_-$および$b_- \in B_-$を格納しており、A_-は$\{a_0, a_1, a_2\}$におけるa_+の補集合であり、B_-は$\{b_0, b_1, b_2\}$におけるb_+の補集合であり、
前記秘密計算装置P_iの共有部と前記秘密計算装置P_+の共有部とが任意値r_+を共有し、
前記秘密計算装置P_iの共有部と前記秘密計算装置P_-の共有部とが任意値r_-を共有し、
前記秘密計算装置P_iの演算部が$c_+ = (a_+ + a_-)(b_+ + b_-) - a_-b_- + r_+ - r_-$を計算し、
前記秘密計算装置P_iの出力部が前記秘密計算装置P_+に対してc_+を出力し、前記秘密計算装置P_+の入力部にc_+が入力される、秘密計算システム。

【請求項２】
秘密計算装置P_0と秘密計算装置P_1と秘密計算装置P_2とを有し、
$i \in \{0, 1, 2\}$であり、P_+が$P_{(i+1) \bmod 3}$であり、P_-が$P_{(i-1) \bmod 3}$であり、$a(n)$，$b(n)$が任意値であり、$a_0(n)$，$a_1(n)$，$a_2(n)$が$a(n)=a_0(n)+a_1(n)+a_2(n)$を満たすサブシェアであり、$b_0(n)$，$b_1(n)$，$b_2(n)$が$b(n)=b_0(n)+b_1(n)+b_2(n)$を満たすサブシェアであり、Nが正整数であり、$n=0, \cdots, N-1$であり、
前記秘密計算装置P_iの記憶部と前記秘密計算装置P_+の記憶部とが前記サブシェア$a_+(n) \in \{a_0(n), a_1(n), a_2(n)\}$および$b_+(n) \in \{b_0(n), b_1(n), b_2(n)\}$を格納しており、
前記秘密計算装置P_iの記憶部と前記秘密計算装置P_-の記憶部とが前記サブシェア$a_-(n) \in A_-(n)$および$b_-(n) \in B_-(n)$を格納しており、$A_-(n)$は$\{a_0(n), a_1(n), a_2(n)\}$における$a_+(n)$の補集合であり、$B_-(n)$は$\{b_0(n), b_1(n), b_2(n)\}$における$b_+(n)$の補集合であり、
前記秘密計算装置P_iの共有部と前記秘密計算装置P_+の共有部とが任意値r_+を共有し、
前記秘密計算装置P_iの共有部と前記秘密計算装置P_-の共有部とが任意値r_-を共有し、
前記秘密計算装置P_iの演算部が
【数６】

$$c_+ = \sum_{n=0}^{N-1}\{(a_+(n)+a_-(n))(b_+(n)+b_-(n)) - a_-(n)b_-(n)+r_+-r_-\}$$

を計算し、
前記秘密計算装置P_iの出力部が前記秘密計算装置P_+に対してc_+を出力し、前記秘密計算装置P_+の入力部にc_+が入力される、秘密計算システム。
【請求項３】
$i \in \{0, 1, 2\}$であり、P_+が$P_{(i+1) \bmod 3}$であり、P_-が$P_{(i-1) \bmod 3}$であり、a，bが任意値であり、a_0，a_1，a_2が$a=a_0+a_1+a_2$を満たすサブシェアであり、b_0，b_1，b_2が$b=b_0+b_1+b_2$を満たすサブシェアであり、
秘密計算装置P_+に格納された前記サブシェア$a_+ \in \{a_0, a_1, a_2\}$および$b_+ \in \{b_0, b_1, b_2\}$、ならびに、秘密計算装置$P_-$に格納された前記サブシェア$a_- \in A_-$および$b_- \in B_-$を格納する記憶部と（ただし、$A_-$は$\{a_0, a_1, a_2\}$における$a_+$の補集合であり、$B_-$は$\{b_0, b_1, b_2\}$における$b_+$の補集合である）、
前記秘密計算装置P_+との間で任意値r_+を共有し、前記秘密計算装置P_-との間で任意値r_-を共有する共有部と、
$c_+=(a_++a_-)(b_++b_-)-a_-b_-+r_+-r_-$を計算する演算部と、
c_+を前記秘密計算装置P_+に対して出力する出力部と、
を有する秘密計算装置。
【請求項４】
$i \in \{0, 1, 2\}$であり、P_+が$P_{(i+1) \bmod 3}$であり、P_-が$P_{(i-1) \bmod 3}$であり、$a(n)$，$b(n)$が任意値であり、$a_0(n)$，$a_1(n)$，$a_2(n)$が$a(n)=a_0(n)+a_1(n)+a_2(n)$を満たすサブシェアであり、$b_0(n)$，$b_1(n)$，$b_2(n)$が$b(n)=b_0(n)+b_1(n)+b_2(n)$を満たすサブシェアであり、
秘密計算装置P_+に格納された前記サブシェア$a_+(n) \in \{a_0(n), a_1(n), a_2(n)\}$および$b_+(n) \in \{b_0(n), b_1(n), b_2(n)\}$、ならびに、秘密計算装置$P_-$に格納された前記サブシェア$a_-(n) \in A_-(n)$および$b_-(n$

）∈Ｂ＿（ｎ）を格納する記憶部と（ただし、Ａ＿（ｎ）は｛ａ０（ｎ），ａ１（ｎ），ａ２（ｎ）｝におけるａ＋（ｎ）の補集合であり、Ｂ＿（ｎ）は｛ｂ０（ｎ），ｂ１（ｎ），ｂ２（ｎ）｝におけるｂ＋（ｎ）の補集合である）、

前記秘密計算装置Ｐ＋との間で任意値ｒ＋を共有し、前記秘密計算装置Ｐ＿との間で任意値ｒ＿を共有する共有部と、

【数７】

$$c_+ = \sum_{n=0}^{N-1}\{(a_+(n)+a_-(n))(b_+(n)+b_-(n)) - a_-(n)b_-(n)+r_+-r_-\}$$

を計算する演算部と、

ｃ＋を前記秘密計算装置Ｐ＋に対して出力する出力部と、

を有する秘密計算装置。

【請求項５】

請求項４の秘密計算装置であって、前記任意値ｒ＋がｒ＋（ｎ）であり、前記任意値ｒ＿がｒ＿（ｎ）である、秘密計算装置。

【請求項６】

ｉ∈｛０，１，２｝であり、Ｐ＋がＰ（ｉ＋１）ｍｏｄ３であり、Ｐ＿がＰ（ｉ－１）ｍｏｄ３であり、ａ，ｂが任意値であり、ａ０，ａ１，ａ２がａ＝ａ０＋ａ１＋ａ２を満たすサブシェアであり、ｂ０，ｂ１，ｂ２がｂ＝ｂ０＋ｂ１＋ｂ２を満たすサブシェアであり、

秘密計算装置Ｐ＋に格納された前記サブシェアａ＋∈｛ａ０，ａ１，ａ２｝およびｂ＋∈｛ｂ０，ｂ１，ｂ２｝、ならびに、秘密計算装置Ｐ＿に格納された前記サブシェアａ＿∈Ａ＿およびｂ＿∈Ｂ＿が秘密計算装置Ｐｉの記憶部に格納されており、Ａ＿は｛ａ０，ａ１，ａ２｝におけるａ＋の補集合であり、Ｂ＿は｛ｂ０，ｂ１，ｂ２｝におけるｂ＋の補集合であり、

前記秘密計算装置Ｐｉの共有部が、前記秘密計算装置Ｐ＋との間で任意値ｒ＋を共有し、前記秘密計算装置Ｐ＿との間で任意値ｒ＿を共有するステップと、

前記秘密計算装置Ｐｉの演算部が、ｃ＋＝（ａ＋＋ａ＿）（ｂ＋＋ｂ＿）－ａ＿ｂ＿＋ｒ＋－ｒ＿を計算するステップと、

前記秘密計算装置Ｐｉの出力部が前記秘密計算装置Ｐ＋に対してｃ＋を出力するステップと、

を有する秘密計算方法。

【請求項７】

ｉ∈｛０，１，２｝であり、Ｐ＋がＰ（ｉ＋１）ｍｏｄ３であり、Ｐ＿がＰ（ｉ－１）ｍｏｄ３であり、ａ（ｎ），ｂ（ｎ）が任意値であり、ａ０（ｎ），ａ１（ｎ），ａ２（ｎ）がａ（ｎ）＝ａ０（ｎ）＋ａ１（ｎ）＋ａ２（ｎ）を満たすサブシェアであり、ｂ０（ｎ），ｂ１（ｎ），ｂ２（ｎ）がｂ（ｎ）＝ｂ０（ｎ）＋ｂ１（ｎ）＋ｂ２（ｎ）を満たすサブシェアであり、

秘密計算装置Ｐ＋に格納された前記サブシェアａ＋（ｎ）∈｛ａ０（ｎ），ａ１（ｎ），ａ２（ｎ）｝およびｂ＋（ｎ）∈｛ｂ０（ｎ），ｂ１（ｎ），ｂ２（ｎ）｝、ならびに、秘密計算装置Ｐ＿に格納された前記サブシェアａ＿（ｎ）∈Ａ＿（ｎ）およびｂ＿（ｎ）∈Ｂ＿（ｎ）が秘密計算装置Ｐｉの記憶部に格納されており、Ａ＿（ｎ）は｛ａ０（ｎ），ａ１（ｎ），ａ２（ｎ）｝におけるａ＋（ｎ）の補集合であり、Ｂ＿（ｎ）は｛ｂ０（ｎ），ｂ１（ｎ），ｂ２（ｎ）｝におけるｂ＋（ｎ）の補集合であり、

前記秘密計算装置Ｐｉの共有部が、前記秘密計算装置Ｐ＋との間で任意値ｒ＋を共有し、前記秘密計算装置Ｐ＿との間で任意値ｒ＿を共有するステップと、

前記秘密計算装置Ｐｉの演算部が、

【数８】

$$c_+ = \sum_{n=0}^{N-1}\{(a_+(n)+a_-(n))(b_+(n)+b_-(n)) - a_-(n)b_-(n)+r_+ - r_-\}$$

を計算するステップと、

前記秘密計算装置P_iの出力部が前記秘密計算装置P_+に対してc_+を出力するステップと、

を有する秘密計算方法。

【請求項８】

請求項３または４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。

【請求項９】

請求項３または４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を格納したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、暗号技術分野に関し、特に秘密計算技術分野に関する。

【背景技術】

【０００２】

複数の秘密計算装置間で値の受け渡しを行い、各秘密計算装置が他の秘密計算装置から受け取った値を用いて秘密乗算や秘密積和などの秘密計算を行う方式がある（例えば、特許文献１等参照）。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特許６００６８４２号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

しかし、特許文献１に記載された方式は加減乗算数回数およびメモリアクセス回数が多いという課題がある。

【０００５】

本発明の目的は、従来よりも少ない加減乗算数回数およびメモリアクセス回数で秘密乗算または秘密積和を行う技術を提供することである。

【課題を解決するための手段】

【０００６】

本発明の秘密乗算は次のように行われる。秘密計算装置P_iの記憶部と秘密計算装置P_+の記憶部とがサブシェア$a_+ \in \{a_0, a_1, a_2\}$および$b_+ \in \{b_0, b_1, b_2\}$を格納しており、秘密計算装置$P_i$の記憶部と秘密計算装置$P_-$の記憶部とがサブシェア$a_- \in A_-$および$b_- \in B_-$を格納している。ただし、$i \in \{0, 1, 2\}$であり、$P_+$が$P_{(i+1) \bmod 3}$であり、$P_-$が$P_{(i-1) \bmod 3}$であり、a，bが任意値であり、$a_0$，$a_1$，$a_2$が$a = a_0 + a_1 + a_2$を満たすサブシェアであり、$b_0$，$b_1$，$b_2$が$b = b_0 + b_1 + b_2$を満たすサブシェアであり、$A_-$は$\{a_0, a_1, a_2\}$における$a_+$の補集合であり、$B_-$は$\{b_0, b_1, b_2\}$における$b_+$の補集合である。秘密計算装置$P_i$の共有部と秘密計算装置$P_+$の共有部とが任意値$r_+$を共有し、秘密計算装置$P_i$の共有部と秘密計算装置$P_-$の共有部とが任意値$r_-$を共有し、秘密計算装置$P_i$の演算部が$c_+ = (a_+ + a_-)(b_+ + b_-) - a_-b_- + r_+ - r_-$を計算する。各秘密計算装置$P_i$の出力部は秘密計算装置$P_+$に対して$c_+$を出力し、秘密計算装置$P_+$の入力部に$c_+$が入力される。

【０００７】
本発明の秘密積和は次のように行われる。秘密計算装置P_iの記憶部と秘密計算装置P_+の記憶部とがサブシェア$a_+(n)\in\{a_0(n), a_1(n), a_2(n)\}$および$b_+(n)\in\{b_0(n), b_1(n), b_2(n)\}$を格納しており、秘密計算装置$P_i$の記憶部と秘密計算装置$P_-$の記憶部とがサブシェア$a_-(n)\in A_-(n)$および$b_-(n)\in B_-(n)$を格納している。ただし、$i\in\{0, 1, 2\}$であり、$P_+$が$P_{(i+1) \bmod 3}$であり、$P_-$が$P_{(i-1) \bmod 3}$であり、$a(n)$，$b(n)$が任意値であり、$a_0(n)$，$a_1(n)$，$a_2(n)$が$a(n)=a_0(n)+a_1(n)+a_2(n)$を満たすサブシェアであり、$b_0(n)$，$b_1(n)$，$b_2(n)$が$b(n)=b_0(n)+b_1(n)+b_2(n)$を満たすサブシェアであり、Nが正整数であり、$n=0, \cdots, N-1$であり、$A_-(n)$は$\{a_0(n), a_1(n), a_2(n)\}$における$a_+(n)$の補集合であり、$B_-(n)$は$\{b_0(n), b_1(n), b_2(n)\}$における$b_+(n)$の補集合である。秘密計算装置$P_i$の共有部と秘密計算装置$P_+$の共有部とが任意値$r_+$を共有し、秘密計算装置$P_i$の共有部と秘密計算装置$P_-$の共有部とが任意値$r_-$を共有し、秘密計算装置$P_i$の演算部が
【数１】

$$c_+ = \sum_{n=0}^{N-1}\{(a_+(n)+a_-(n))(b_+(n)+b_-(n)) - a_-(n)b_-(n)+r_+-r_-\}$$

を計算する。各秘密計算装置P_iは秘密計算装置P_+に対してc_+を出力し、秘密計算装置P_+の入力部にc_+が入力される。
【発明の効果】
【０００８】
これにより、従来よりも少ない加減乗算数回数およびメモリアクセス回数で秘密乗算または秘密積和を行うことができる。
【図面の簡単な説明】
【０００９】
【図１】図１は実施形態の秘密計算システムを例示したブロック図である。
【図２】図２は実施形態の秘密計算装置を例示したブロック図である。
【図３】図３は実施形態の秘密乗算を説明するための概念図である。
【図４】図４は実施形態の秘密計算方法を説明するためのフロー図である。
【図５】図５は実施形態の秘密積和を説明するための概念図である。
【図６】図６は実施形態の秘密計算方法を説明するためのフロー図である。
【発明を実施するための形態】
【００１０】
以下、図面を用いて本発明の実施形態を説明する。
【００１１】
［第１実施形態］
第１実施形態では、任意値ａ，ｂ∈Ｆの乗算ａｂ∈Ｆを秘密計算で行う（秘密乗算）。ただし、Ｆは有限体を表す。この秘密乗算では、任意値ａの秘密分散値（シェア）と任意値ｂの秘密分散値とから乗算結果ａｂの秘密分散値を得る。以下に詳細に説明する。
【００１２】
＜構成＞
図１に例示するように、本形態の秘密計算システム１は、３個の秘密計算装置１１－P_0，１１－P_1，１１－P_2（秘密計算装置P_0，P_1，P_2）を有する。秘密計算装置１１－P_0，１１－P_1，１１－P_2は、インターネットなどの通信網を通じた通信が可能なように構成されている。図２に例示するように、本形態の秘密計算装置１１－Ｐ（ただし、$P\in\{P_0, P_1, P_2\}$）は、記憶部１１１－Ｐ（ストレージおよびメモリ）、演算部１１２－Ｐ、制御部１１３－Ｐ、共有部１１４－Ｐ、および通信部１１５－Ｐを有

する。秘密計算装置１１－Ｐは、制御部１１３－Ｐの制御のもとで各処理を実行し、各処理で得られたデータは、逐一、記憶部１１１－Ｐに格納され、必要に応じて読み出される。

【００１３】

＜事前処理＞

事前処理により、任意値ａが$a=a_0+a_1+a_2\in F$を満たすサブシェア$a_0, a_1, a_2\in F$に秘密分散されており、任意値ｂが$b=b_0+b_1+b_2\in F$を満たすサブシェア$b_0, b_1, b_2\in F$に秘密分散されている。秘密計算装置$11-P_i$の記憶部$11-P_i$はサブシェア$a_+\in\{a_0, a_1, a_2\}$および$b_+\in\{b_0, b_1, b_2\}$を格納しており、秘密計算装置$11-P_+$の記憶部$111-P_+$もサブシェアa_+およびb_+を格納している。サブシェアa_+は$\{a_0, a_1, a_2\}$の何れか１つの要素であり、サブシェアb_+は$\{b_0, b_1, b_2\}$の何れか１つの要素である。秘密計算装置$11-P_i$の記憶部$111-P_i$はサブシェア$a_-\in A_-$および$b_-\in B_-$を格納しており、秘密計算装置$11-P_-$の記憶部$111-P_-$もサブシェアa_-およびb_-を格納している。サブシェアa_-はA_-の何れか１つの要素であり、サブシェアb_-はB_-の何れか１つの要素である。ただし、A_-は$\{a_0, a_1, a_2\}$におけるa_+の補集合であり（$A_-=\{a_0, a_1, a_2\}-\{a_+\}$）、$B_-$は$\{b_0, b_1, b_2\}$における$b_+$の補集合である（$B_-=\{b_0, b_1, b_2\}-\{b_+\}$）。また、$i\in\{0, 1, 2\}$であり、$P_+$は$P_{(i+1) \bmod 3}$であり、$P_-$は$P_{(i-1) \bmod 3}$である。図３の例では、秘密計算装置$11-P_0$の記憶部$111-P_0$にサブシェア（$a_0, a_1$）および（$b_0, b_1$）が格納されており、秘密計算装置$11-P_1$の記憶部$111-P_1$にサブシェア（$a_1, a_2$）および（$b_1, b_2$）が格納されており、秘密計算装置$11-P_2$の記憶部$111-P_2$にサブシェア（$a_2, a_0$）および（$b_2, b_0$）が格納されている。なお、（$a_0, a_1$）（$a_1, a_2$）（$a_2, a_0$）はａの秘密分散値であり、（$b_0, b_1$）（$b_1, b_2$）（$b_2, b_0$）はｂの秘密分散値である。

【００１４】

＜秘密計算＞

この事前処理が行われたことを前提に、各秘密計算装置$11-P_i$（ただし、$i\in\{0, 1, 2\}$）は以下の秘密計算を行う（図３および図４）。

【００１５】

各秘密計算装置$11-P_i$の共有部$114-P_i$と秘密計算装置$11-P_+$の共有部$114-P_+$とが任意値$r_+\in F$を共有する。すなわち、共有部$114-P_i$および共有部$114-P_+$は互いに同一の任意値r_+を得る。共有された任意値r_+は記憶部$111-P_i$および記憶部$111-P_+$に格納される。任意値r_+の例は、擬似乱数、真正乱数、予め定められた複数の値から選択された値、入力値、別処理で得られた値などである。任意値r_+の共有は公知の方法によって実現できる。例えば、共有部$114-P_i$から共有部$114-P_+$に任意値r_+または任意値r_+を特定するための情報を送ることで、共有部$114-P_i$と共有部$114-P_+$との間で任意値r_+が共有されてもよい。逆に、共有部$114-P_+$から共有部$114-P_i$に任意値r_+または任意値r_+を特定するための情報を送ることで、共有部$114-P_i$と共有部$114-P_+$との間で任意値r_+が共有されてもよい。予め共有部$114-P_i$と共有部$114-P_+$との間でシード値を共有しておき、共有部$114-P_i$および共有部$114-P_+$がこのシード値を用いて予め定められた処理を行うことで、共有部$114-P_i$と共有部$114-P_+$との間で任意値r_+が共有されてもよい。公知の鍵交換アルゴリズムを用いて共有部$114-P_i$と共有部$114-P_+$との間で任意値r_+が共有されてもよい（ステップＳ１１）。

【００１６】

各秘密計算装置$11-P_i$の共有部$114-P_i$と秘密計算装置$11-P_-$の共有部$114-P_-$とが任意値$r_-\in F$を共有する。すなわち、共有部$114-P_i$および共有部$114-P_-$は互いに同一の任意値r_-を得る。共有された任意値r_-は記憶部$111-P_i$および記憶部$111-P_-$に格納される。任意値r_-の例は、擬似乱数、真正乱数、

予め定められた複数の値から選択された値、入力値、別処理で得られた値などである。任意値$r_{_}$の共有は公知の方法によって実現できる。例えば、共有部１１４－P_iから共有部１１４－$P_{_}$に任意値$r_{_}$または任意値$r_{_}$を特定するための情報を送ることで、共有部１１４－P_iと共有部１１４－$P_{_}$との間で任意値$r_{_}$が共有されてもよい。逆に、共有部１１４－$P_{_}$から共有部１１４－P_iに任意値$r_{_}$または任意値$r_{_}$を特定するための情報を送ることで、共有部１１４－P_iと共有部１１４－$P_{_}$との間で任意値$r_{_}$が共有されてもよい。あるいは、予め共有部１１４－P_iと共有部１１４－$P_{_}$との間でシード値を共有しておき、共有部１１４－P_iおよび共有部１１４－$P_{_}$がこのシード値を用いて予め定められた処理を行うことで、共有部１１４－P_iと共有部１１４－$P_{_}$との間で任意値$r_{_}$が共有されてもよい。公知の鍵交換アルゴリズムを用いて共有部１１４－P_iと共有部１１４－$P_{_}$との間で任意値$r_{_}$が共有されてもよい（ステップＳ１２）。

【００１７】

図３の例では、ステップＳ１１およびＳ１２の処理により、共有部１１４－P_0と共有部１１４－P_1とが任意値$r_{01}\in F$を共有し、共有部１１４－P_1と共有部１１４－P_2とが任意値$r_{12}\in F$を共有し、共有部１１４－P_2と共有部１１４－P_0とが任意値$r_{20}\in F$を共有する。

【００１８】

各秘密計算装置１１－P_iの演算部１１２－P_iが、記憶部１１１－Pから読み込んだa_+，$a_{\_}$，b_+，$b_{\_}$，r_+，$r_{_}$を用い、$c_+=(a_++a_{_})(b_++b_{_})-a_{_}b_{_}+r_+-r_{_}\in F$を計算して出力する。図３の例では、秘密計算装置１１－P_0の演算部１１２－P_0が$c_1=(a_0+a_1)(b_0+b_1)-a_0b_0+r_{01}-r_{20}\in F$を計算して出力し、秘密計算装置１１－$P_1$の演算部１１２－$P_1$が$c_2=(a_1+a_2)(b_1+b_2)-a_1b_1+r_{12}-r_{01}\in F$を計算して出力し、秘密計算装置１１－$P_2$の演算部１１２－$P_2$が$c_0=(a_2+a_0)(b_2+b_0)-a_2b_2+r_{20}-r_{12}\in F$を計算して出力する（ステップＳ１３）。

【００１９】

各秘密計算装置１１－P_iの通信部１１５－P_iは秘密計算装置１１－P_+に対してc_+を送信する（c_+を出力する）（ステップＳ１４）。c_+は秘密計算装置１１－P_+の通信部１１５－P_+で受信（入力）される。秘密計算装置１１－$P_{_}$の演算部１１２－$P_{_}$で計算されて通信部１１５－$P_{_}$から送信された値を$c_{_}$と表記すると、各秘密計算装置１１－P_iの通信部１１５－P_iは$c_{_}$を受信する（ステップＳ１５）。図３の例では、秘密計算装置１１－P_0の通信部１１５－P_0が秘密計算装置１１－P_1に対してc_1を送信し、c_1が秘密計算装置１１－P_1の通信部１１５－P_1で受信される。秘密計算装置１１－P_1の通信部１１５－P_1が秘密計算装置１１－P_2に対してc_2を送信し、c_2が秘密計算装置１１－P_2の通信部１１５－P_2で受信される。秘密計算装置１１－P_2の通信部１１５－P_2が秘密計算装置１１－P_0に対してc_0を送信し、c_0が秘密計算装置１１－P_0の通信部１１５－P_0で受信される（ステップＳ１４，Ｓ１５）。

【００２０】

ステップＳ１５で受信された$c_{_}$、および、ステップＳ１３で得られたc_+は、各秘密計算装置１１－P_iの記憶部１１１－P_iに格納される。図３の例では、（c_0，c_1）が秘密計算装置１１－P_0の記憶部１１１－P_0に格納され、（c_1，c_2）が秘密計算装置１１－P_1の記憶部１１１－P_1に格納され、（c_2，c_0）が秘密計算装置１１－P_2の記憶部１１１－P_2に格納される。

【００２１】

本形態のc_0，c_1，c_2は$ab=c_0+c_1+c_2\in F$を満たす乗算結果abのサブシェアであり、（c_0，c_1）（c_1，c_2）（c_2，c_0）は乗算結果abの秘密分散値である。これらの秘密分散値（c_0，c_1）（c_1，c_2）（c_2，c_0）の何れか２個が得られれば乗算結果abを復元できる。すなわち、$c_0+c_1+c_2=ab$を満たす。図３の例では、

$c_0+c_1+c_2$

$=(a_0+a_1)(b_0+b_1)-a_0b_0+r_{01}-r_{20}+(a_1+a_2)(b_1+b_2)-a_1b_1+r_{12}-r_{01}+(a_2+a_0)(b_2+b_0)-a_2b_2+r_{20}-r_{12}$
$=a_0b_1+a_1b_0+a_1b_1+a_1b_2+a_2b_1+a_2b_2+a_2b_0+a_0b_2+a_0b_0$
$=(a_0+a_1+a_2)(b_0+b_1+b_2)$
$=ab$
となる。

【００２２】

各秘密計算装置１１－P_iの記憶部１１１－P_iに格納された（c_-，c_+）はさらに別の秘密計算装置（図示せず）の入力とされてもよいし、乗算結果ａｂの復元を行う復元装置（図示せず）の入力とされて乗算結果ａｂが復元されて出力されてもよい。

【００２３】

＜本形態の特徴＞

以上のように本形態では、特許文献１に記載された従来方式よりも少ない加減乗算数回数およびメモリアクセス回数で秘密乗算を行うことができる。すなわち、特許文献１に記載された従来方式では、各秘密計算装置は、メモリに格納された秘密分散値等を用いて自ら加減乗算を行って得た値をメモリに保存しておき、他の秘密計算装置で加減乗算を行って得られた値を受信してメモリに保存し、メモリに保存されたこれらの値を用いてさらに加減乗算を行う必要があった。そのため、特許文献１の方式は、加減乗算数回数およびメモリアクセス回数が多かった。これに対し、本形態では、メモリに格納された秘密分散値等を用いて自ら加減乗算を行って得た値、および、他の秘密計算装置で加減乗算を行って得られた値がそのまま演算結果のサブシェアとなるため、特許文献１の方式よりも加減乗算数回数およびメモリアクセス回数が少ない。特に、演算速度の速い秘密計算ではメモリへのアクセス時間が全体の演算速度を向上する上でのボトルネックとなるが、本形態の方式ではメモリアクセス回数を削減できるため、演算速度を大幅に向上できる。例えば、従来技術の秘密乗算では、$c_{XY}=a_-b_++a_+b_--r_{ZX}$を計算するときに$a_-$，$b_+$，$a_+$，$b_-$を読み込み、得られた$c_{XY}$を書き込む。これには乗算を２回、加減算を２回行う必要がある。さらに、従来技術の秘密乗算では、$c_-=a_-b_-+c_{ZX}+r_{ZX}$を計算するときにa_-，b_-，c_{ZX}を読み込み、c_-を書き込む。これには乗算を１回、加減算を３回行う必要がある。またさらに、従来技術の秘密乗算では、$c_+=a_+b_++c_{XY}+r_{XY}$を計算するときにa_+，b_+，c_{XY}を読み込み、得られたc_+を書き込む。これには乗算を１回、加減算を３回行う必要がある。そのため、パーティあたりで合計、読込を１０回、書込を３回、乗算を４回、加減算を８回行う必要があった。これに対し、本形態の場合、秘密計算装置１０－P_iは$c_+=(a_++a_-)(b_++b_-)-a_-b_-+r_+-r_-$を計算するときに$a_-$，$b_+$，$a_+$，$b_-$を読み込み、得られた$c_+$を書き込む。そのため、パーティあたり、合計で読込４回、書込１回、乗算２回、加減算５回を行えばよい。従来技術と比較した場合、本形態では読込回数を４０％、書込回数を３３％、乗算回数を５０％、加減算回数を６３％にできる。

【００２４】

［第２実施形態］

第２実施形態では、任意値ａ（０），…，ａ（Ｎ－１）およびｂ（０），…，ｂ（Ｎ－１）に対する積和ａ（０）ｂ（０）＋…＋ａ（Ｎ－１）ｂ（Ｎ－１）∈Ｆを秘密計算で行う（秘密積和）。ただし、Ｆは有限体を表し、Ｎは正整数（例えば、２以上の整数）である。この秘密積和では、ｎ＝０，…，Ｎ－１についての任意値ａ（ｎ）の秘密分散値と任意値ｂ（ｎ）の秘密分散値とから積和結果ａ（０）ｂ（０）＋…＋ａ（Ｎ－１）ｂ（Ｎ－１）の秘密分散値を得る。以下に詳細に説明する。

【００２５】

＜構成＞

図１に例示するように、本形態の秘密計算システム２は、３個の秘密計算装置２１－P

$_0$，２１－Ｐ$_1$，２１－Ｐ$_2$（秘密計算装置Ｐ$_0$，Ｐ$_1$，Ｐ$_2$）を有する。秘密計算装置２１－Ｐ$_0$，２１－Ｐ$_1$，２１－Ｐ$_2$は、インターネットなどの通信網を通じた通信が可能なように構成されている。図２に例示するように、本形態の秘密計算装置２１－Ｐ（ただし、Ｐ∈｛Ｐ$_0$，Ｐ$_1$，Ｐ$_2$｝）は、記憶部２１１－Ｐ（ストレージおよびメモリ）、演算部２１２－Ｐ、制御部２１３－Ｐ、共有部１１４－Ｐ、および通信部１１５－Ｐを有する。秘密計算装置２１－Ｐは、制御部２１３－Ｐの制御のもとで各処理を実行し、各処理で得られたデータは、逐一、記憶部２１１－Ｐに格納され、必要に応じて読み出される。

【００２６】

＜事前処理＞

事前処理により、ｎ＝０，…，Ｎ－１（ただし、Ｎは正整数、例えば、Ｎは２以上の整数）についての任意値ａ（ｎ）がａ（ｎ）＝ａ$_0$（ｎ）＋ａ$_1$（ｎ）＋ａ$_2$（ｎ）∈Ｆを満たすサブシェアａ$_0$（ｎ），ａ$_1$（ｎ），ａ$_2$（ｎ）∈Ｆに秘密分散されており、任意値ｂ（ｎ）がｂ（ｎ）＝ｂ$_0$（ｎ）＋ｂ$_1$（ｎ）＋ｂ$_2$（ｎ）∈Ｆを満たすサブシェアｂ$_0$（ｎ），ｂ$_1$（ｎ），ｂ$_2$（ｎ）∈Ｆに秘密分散されている。秘密計算装置２１－Ｐ$_i$の記憶部２１１－Ｐ$_i$は、ｎ＝０，…，Ｎ－１についてのサブシェアａ$_+$（ｎ）∈｛ａ$_0$（ｎ），ａ$_1$（ｎ），ａ$_2$（ｎ）｝およびｂ$_+$（ｎ）∈｛ｂ$_0$（ｎ），ｂ$_1$（ｎ），ｂ$_2$（ｎ）｝を格納しており、秘密計算装置２１－Ｐ$_+$の記憶部２１１－Ｐ$_+$も、ｎ＝０，…，Ｎ－１についてのサブシェアａ$_+$（ｎ）およびｂ$_+$（ｎ）を格納している。各サブシェアａ$_+$（ｎ）は｛ａ$_0$（ｎ），ａ$_1$（ｎ），ａ$_2$（ｎ）｝の何れか１つの要素であり、各サブシェアｂ$_+$（ｎ）は｛ｂ$_0$（ｎ），ｂ$_1$（ｎ），ｂ$_2$（ｎ）｝の何れか１つの要素である。秘密計算装置２１－Ｐ$_i$の記憶部２１１－Ｐ$_i$は、ｎ＝０，…，Ｎ－１についてのサブシェアａ$_-$（ｎ）∈Ａ$_-$（ｎ）およびｂ$_-$（ｎ）∈Ｂ$_-$（ｎ）を格納しており、秘密計算装置２１－Ｐ$_-$の記憶部２１１－Ｐ$_-$も、ｎ＝０，…，Ｎ－１についてのサブシェアａ$_-$（ｎ）およびｂ$_-$（ｎ）を格納している。各サブシェアａ$_-$（ｎ）はＡ$_-$（ｎ）の何れか１つの要素であり、各サブシェアｂ$_-$（ｎ）はＢ$_-$（ｎ）の何れか１つの要素である。ただし、Ａ$_-$（ｎ）は｛ａ$_0$（ｎ），ａ$_1$（ｎ），ａ$_2$（ｎ）｝におけるａ$_+$（ｎ）の補集合であり（Ａ$_-$（ｎ）＝｛ａ$_0$（ｎ），ａ$_1$（ｎ），ａ$_2$（ｎ）｝－｛ａ$_+$（ｎ）｝）、Ｂ$_-$（ｎ）は｛ｂ$_0$（ｎ），ｂ$_1$（ｎ），ｂ$_2$（ｎ）｝におけるｂ$_+$（ｎ）の補集合である（Ｂ$_-$（ｎ）＝｛ｂ$_0$（ｎ），ｂ$_1$（ｎ），ｂ$_2$（ｎ）｝－｛ｂ$_+$（ｎ）｝）。また、ｉ∈｛０，１，２｝であり、Ｐ$_+$はＰ$_{(i+1) \bmod 3}$であり、Ｐ$_-$はＰ$_{(i-1) \bmod 3}$である。図５の例では、秘密計算装置２１－Ｐ$_0$の記憶部２１１－Ｐ$_0$に、ｎ＝０，…，Ｎ－１についてのサブシェア（ａ$_0$（ｎ），ａ$_1$（ｎ））および（ｂ$_0$（ｎ），ｂ$_1$（ｎ））が格納されており、秘密計算装置２１－Ｐ$_1$の記憶部２１１－Ｐ$_1$に、ｎ＝０，…，Ｎ－１についてのサブシェア（ａ$_1$（ｎ），ａ$_2$（ｎ））および（ｂ$_1$（ｎ），ｂ$_2$（ｎ））が格納されており、秘密計算装置２１－Ｐ$_2$の記憶部２１１－Ｐ$_2$に、ｎ＝０，…，Ｎ－１についてのサブシェア（ａ$_2$（ｎ），ａ$_0$（ｎ））および（ｂ$_2$（ｎ），ｂ$_0$（ｎ））が格納されている。なお、（ａ$_0$（ｎ），ａ$_1$（ｎ））（ａ$_1$（ｎ），ａ$_2$（ｎ））（ａ$_2$（ｎ），ａ$_0$（ｎ））はａ（ｎ）の秘密分散値であり、（ｂ$_0$（ｎ），ｂ$_1$（ｎ））（ｂ$_1$（ｎ），ｂ$_2$（ｎ））（ｂ$_2$（ｎ），ｂ$_0$（ｎ））はｂ（ｎ）の秘密分散値である。

【００２７】

＜秘密計算＞

この事前処理が行われたことを前提に、各秘密計算装置２１－Ｐ$_i$（ただし、ｉ∈｛０，１，２｝）は以下の秘密計算を行う（図５および図６）。

【００２８】

各秘密計算装置２１－Ｐ$_i$の共有部１１４－Ｐ$_i$と秘密計算装置２１－Ｐ$_+$の共有部１１４－Ｐ$_+$とが任意値ｒ$_+$∈Ｆを共有する。共有された任意値ｒ$_+$は記憶部２１１－Ｐ$_i$および記憶部２１１－Ｐ$_+$に格納される。任意値ｒ$_+$およびその共有処理の具体例は第１実施形態で説明した通りである（ステップＳ２１）。

【００２９】
各秘密計算装置２１－Ｐ$_i$の共有部１１４－Ｐ$_i$と秘密計算装置２１－Ｐ$_-$の共有部１１４－Ｐ$_-$とが任意値ｒ$_-$∈Ｆを共有する。共有された任意値ｒ$_-$は記憶部２１１－Ｐ$_i$および記憶部２１１－Ｐ$_-$に格納される。任意値ｒ$_-$およびその共有処理の具体例は第１実施形態で説明した通りである（ステップＳ２２）。
【００３０】
図５の例では、ステップＳ２１およびＳ２２の処理により、共有部１１４－Ｐ$_0$と共有部１１４－Ｐ$_1$とが任意値ｒ$_{01}$∈Ｆを共有し、共有部１１４－Ｐ$_1$と共有部１１４－Ｐ$_2$とが任意値ｒ$_{12}$∈Ｆを共有し、共有部１１４－Ｐ$_2$と共有部１１４－Ｐ$_0$とが任意値ｒ$_{20}$∈Ｆを共有する。
【００３１】
各秘密計算装置２１－Ｐ$_i$の演算部２１２－Ｐ$_i$が、記憶部２１１－Ｐ$_i$から読み込んだ、ｎ＝０，…，Ｎ－１についてのａ$_+$（ｎ），ａ$_-$（ｎ），ｂ$_+$（ｎ），ｂ$_-$（ｎ），ｒ$_+$，ｒ$_-$を用い、
【数２】
$$c_+ = \sum_{n=0}^{N-1}\{(a_+(n)+a_-(n))(b_+(n)+b_-(n)) - a_-(n)b_-(n)+r_+ - r_-\} \in F$$
を計算して出力する。図５の例では、秘密計算装置２１－Ｐ$_0$の演算部２１２－Ｐ$_0$が
【数３】
$$c_1 = \sum_{n=0}^{N-1}\{(a_0(n)+a_1(n))(b_0(n)+b_1(n)) - a_0(n)b_0(n)+r_{01} - r_{20}\} \in F$$
を計算して出力し、秘密計算装置２１－Ｐ$_1$の演算部２１２－Ｐ$_1$が
【数４】
$$c_2 = \sum_{n=0}^{N-1}\{(a_1(n)+a_2(n))(b_1(n)+b_2(n)) - a_1(n)b_1(n)+r_{12} - r_{01}\} \in F$$
を計算して出力し、秘密計算装置２１－Ｐ$_2$の演算部２１２－Ｐ$_2$が
【数５】
$$c_0 = \sum_{n=0}^{N-1}\{(a_2(n)+a_0(n))(b_2(n)+b_0(n)) - a_2(n)b_2(n)+r_{20} - r_{12}\} \in F$$
を計算して出力する（ステップＳ２３）。
【００３２】
各秘密計算装置２１－Ｐ$_i$の通信部１１５－Ｐ$_i$は秘密計算装置２１－Ｐ$_+$に対してｃ$_+$を送信する（ｃ$_+$を出力する）（ステップＳ２４）。ｃ$_+$は秘密計算装置２１－Ｐ$_+$の通信部１１５－Ｐ$_+$で受信（入力）される。秘密計算装置２１－Ｐ$_-$の演算部２１２－Ｐ$_-$で計算されて通信部１１５－Ｐ$_-$から送信された値をｃ$_-$と表記すると、各秘密計算装置２１－Ｐ$_i$の通信部１１５－Ｐ$_i$はｃ$_-$を受信する（ステップＳ２５）。図５の例では、秘密計算装置２１－Ｐ$_0$の通信部１１５－Ｐ$_0$が秘密計算装置２１－Ｐ$_1$に対してｃ$_1$を送信し、ｃ$_1$が秘密計算装置２１－Ｐ$_1$の通信部１１５－Ｐ$_1$で受信される。秘密計算

装置２１－P_1の通信部１１５－P_1が秘密計算装置２１－P_2に対してc_2を送信し、c_2が秘密計算装置２１－P_2の通信部１１５－P_2で受信される。秘密計算装置２１－P_2の通信部１１５－P_2が秘密計算装置２１－P_0に対してc_0を送信し、c_0が秘密計算装置２１－P_0の通信部１１５－P_0で受信される（ステップＳ２４，Ｓ２５）。

【００３３】

ステップＳ２５で受信されたc_-、および、ステップＳ２３で得られたc_+は、各秘密計算装置２１－P_iの記憶部２１１－P_iに格納される。図５の例では、（c_0，c_1）が秘密計算装置２１－P_0の記憶部２１１－P_0に格納され、（c_1，c_2）が秘密計算装置２１－P_1の記憶部２１１－P_1に格納され、（c_2，c_0）が秘密計算装置２１－P_2の記憶部２１１－P_2に格納される。

【００３４】

本形態のc_0，c_1，c_2は$a(0)b(0)+\cdots+a(N-1)b(N-1)=c_0+c_1+c_2 \in F$を満たす積和結果$a(0)b(0)+\cdots+a(N-1)b(N-1)$のサブシェアである。（$c_0$，$c_1$）（$c_1$，$c_2$）（$c_2$，$c_0$）は積和結果$a(0)b(0)+\cdots+a(N-1)b(N-1)$の秘密分散値である。これらの秘密分散値（$c_0$，$c_1$）（$c_1$，$c_2$）（$c_2$，$c_0$）の何れか２個が得られれば積和結果$a(0)b(0)+\cdots+a(N-1)b(N-1)$を復元できる。すなわち、$c_0+c_1+c_2=a(0)b(0)+\cdots+a(N-1)b(N-1)$を満たす。

【００３５】

各秘密計算装置２１－P_iの記憶部２１１－P_iに格納された（c_-，c_+）はさらに別の秘密計算装置（図示せず）の入力とされてもよいし、積和結果$a(0)b(0)+\cdots+a(N-1)b(N-1)$の復元を行う復元装置（図示せず）の入力とされて積和結果$a(0)b(0)+\cdots+a(N-1)b(N-1)$が復元されて出力されてもよい。

【００３６】

＜本形態の特徴＞

以上のように本形態では、特許文献１に記載された従来方式よりも少ない加減乗算数回数およびメモリアクセス回数で秘密積和を行うことができる。

【００３７】

なお、本発明は上述の実施の形態に限定されるものではない。例えば、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。また、第２実施形態の任意値r_+が$n=0,\cdots,N-1$のそれぞれに対応する$r_+(n)$であってもよいし、任意値r_-が$n=0,\cdots,N-1$のそれぞれに対応する$r_-(n)$であってもよい。例えば、図５の例において、任意値r_{01}が$n=0,\cdots,N-1$のそれぞれに対応する$r_{01}(n) \in F$であってもよいし、任意値r_{20}が$n=0,\cdots,N-1$のそれぞれに対応する$r_{20}(n) \in F$であってもよい。

【００３８】

上記の各装置は、例えば、ＣＰＵ（central processing unit）等のプロセッサ（ハードウェア・プロセッサ）およびＲＡＭ（random-access memory）・ＲＯＭ（read-only memory）等のメモリ等を備える汎用または専用のコンピュータが所定のプログラムを実行することで構成される。このコンピュータは１個のプロセッサやメモリを備えていてもよいし、複数個のプロセッサやメモリを備えていてもよい。このプログラムはコンピュータにインストールされてもよいし、予めＲＯＭ等に記録されていてもよい。また、ＣＰＵのようにプログラムが読み込まれることで機能構成を実現する電子回路（circuitry）ではなく、プログラムを用いることなく処理機能を実現する電子回路を用いて一部またはすべての処理部が構成されてもよい。１個の装置を構成する電子回路が複数のＣＰＵを含んでいてもよい。

【００３９】

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。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。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の例は、非一時的な（non-transitory）記録媒体である。このような記録媒体の例は、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等である。

【００４０】

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。

【００４１】

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。処理の実行時、このコンピュータは、自己の記憶装置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。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。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。

【００４２】

コンピュータ上で所定のプログラムを実行させて本装置の処理機能が実現されるのではなく、これらの処理機能の少なくとも一部がハードウェアで実現されてもよい。

【符号の説明】

【００４３】

１，２　秘密計算システム

１１－Ｐ　秘密計算装置

【図１】

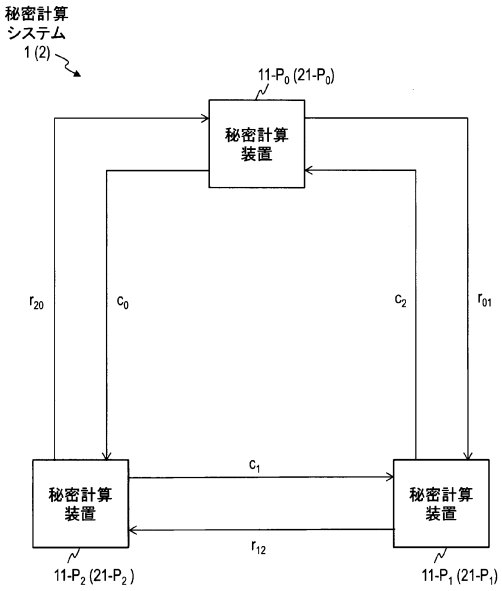

図1

【図２】

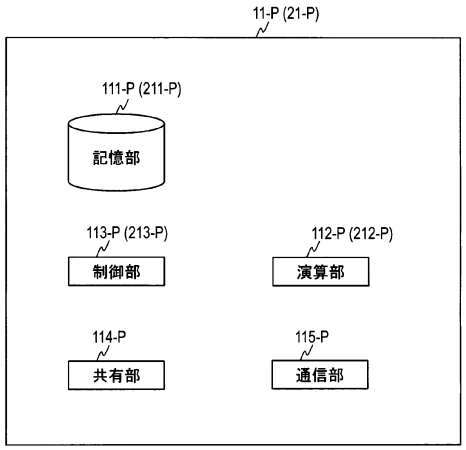

図2

【図３】

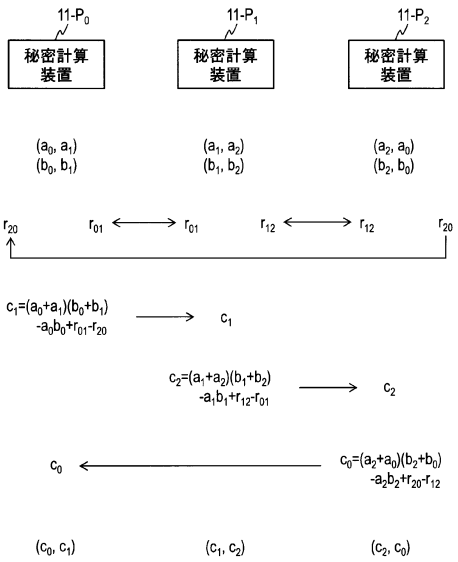

図3

【図４】

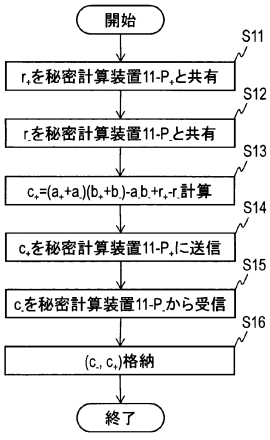

図4

【図５】

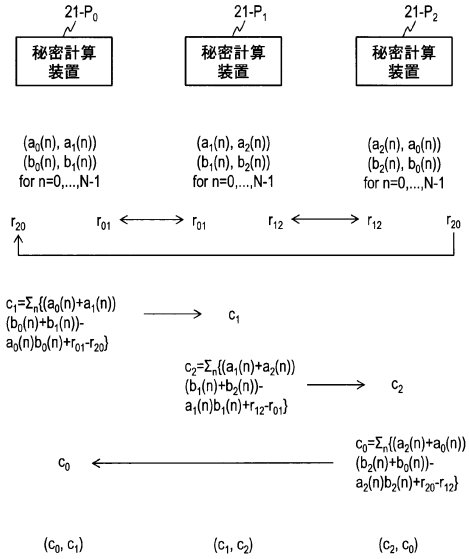
21-P0
21-P1
21-P2
秘密計算装置
秘密計算装置
秘密計算装置
(a0(n), a1(n))
(b0(n), b1(n))
for n=0,...,N-1
(a1(n), a2(n))
(b1(n), b2(n))
for n=0,...,N-1
(a2(n), a0(n))
(b2(n), b0(n))
for n=0,...,N-1
r20
r01
r01
r12
r12
r20
c1=Σn{(a0(n)+a1(n))(b0(n)+b1(n))-a0(n)b0(n)+r01-r20}
c1
c2=Σn{(a1(n)+a2(n))(b1(n)+b2(n))-a1(n)b1(n)+r12-r01}
c2
c0
c0=Σn{(a2(n)+a0(n))(b2(n)+b0(n))-a2(n)b2(n)+r20-r12}
(c0, c1)
(c1, c2)
(c2, c0)

図5

【図６】

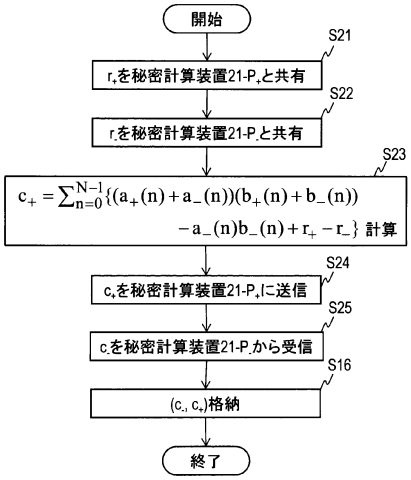
開始
S21
r+を秘密計算装置21-P+と共有
S22
r-を秘密計算装置21-P-と共有
S23
c+ = Σn=0N−1{(a+(n) + a−(n))(b+(n) + b−(n)) − a−(n)b−(n) + r+ − r−} 計算
S24
c+を秘密計算装置21-P+に送信
S25
c-を秘密計算装置21-P-から受信
S16
(c-, c+)格納
終了

図6

フロントページの続き

(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

審査官　金沢　史明

(56)参考文献　特開２０１２－７８４４６（ＪＰ，Ａ）
特許第６００６８４２（ＪＰ，Ｂ１）
特開２０１７－２６７８８（ＪＰ，Ａ）
滝 雄太郎，他，軽量Nパーティ秘匿関数計算の一般解と情報銀行の分散型セキュアストレージへの応用，マルチメディア，分散，協調とモバイル（ＤＩＣＯＭＯ２０１７）シンポジウム論文集，日本，情報処理学会，２０１７年　6月２１日，pp. 779-784

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