

(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
2011年7月21日(21.07.2011)

PCT

(10) 国際公開番号
WO 2011/086992 A1

- (51) 国際特許分類:
G09C 1/00 (2006.01) H04L 9/20 (2006.01)
- (21) 国際出願番号: PCT/JP2011/050278
- (22) 国際出願日: 2011年1月11日(11.01.2011)
- (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 2010-003924 2010年1月12日(12.01.2010) JP
特願 2010-007835 2010年1月18日(18.01.2010) JP
- (71) 出願人(米国を除く全ての指定国について): 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二丁目3番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 山本 剛(YAMAMOTO, Go) [JP/JP]; 〒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). 小林 鉄太郎(KOBAYASHI, Tetsutaro) [JP/JP]; 〒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).

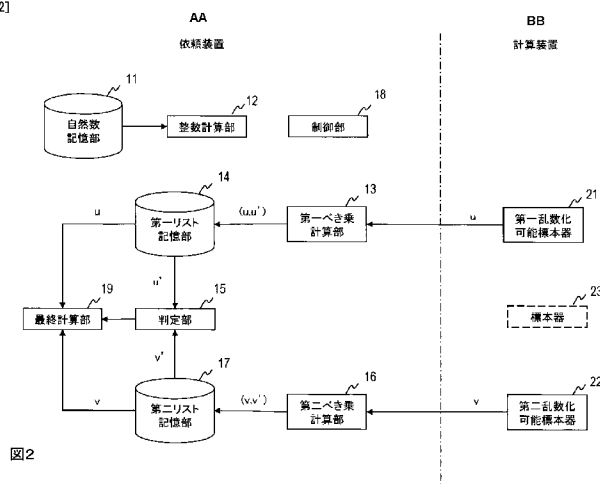
- (74) 代理人: 中尾 直樹, 外(NAKAO, Naoki et al.); 〒1600022 東京都新宿区新宿三丁目1番22号 新宿NSビル4階 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, 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, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, 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

[続葉有]

(54) Title: REPRESENTATIVE CALCULATION SYSTEM, METHOD, REQUEST DEVICE, PROGRAM AND RECORDING MEDIUM

(54) 発明の名称: 代理計算システム、方法、依頼装置、プログラム及びその記録媒体

[図2]



- AA REQUEST DEVICE
BB CALCULATION UNIT
11 NATURAL NUMBER STORAGE UNIT
12 INTEGER CALCULATION UNIT
13 FIRST EXPONENT CALCULATION UNIT
14 FIRST LIST STORAGE UNIT
15 DETERMINING UNIT
16 SECOND EXPONENT CALCULATION UNIT
17 SECOND LIST STORAGE UNIT
18 CONTROL UNIT
19 FINAL CALCULATION UNIT
21 FIRST RANDOMIZABLE SAMPLING UNIT
22 SECOND RANDOMIZABLE SAMPLING UNIT
23 SAMPLING UNIT

(57) Abstract: Using a calculating device with low probability of performing a correct calculation, the function $f(x)$ is calculated. Given G, H are cyclic groups, the function f copies the original x of group H to group G , X_1 and X_2 are stochastic variables having a value in group G , an instance of the stochastic variable X_1 is x_1 and an instance of the stochastic variable X_2 is x_2 , an integer calculation unit uses natural numbers a and b , which are co-prime to each other, to calculate the integers a', b' that satisfy the relation $a'a + b'b = 1$. A first randomizable sample unit may calculate $f(x)^b X_1$ and return the result as u ; a first exponent calculation unit calculates $u' = Ua$; a second randomizable sample unit may calculate $f(x)^a X_2$ and returns the result as v ; a second exponent calculation unit calculates $v' = v^b$; a determining unit determines whether $u' = v'$; a final calculation unit calculates $u^{b'}$, $v^{a'}$ when the determining unit determines that $u' = v'$.

(57) 要約: 正しい計算を行う確率が低い計算装置を用いて関数 $f(x)$ の計算をする。 G, H を巡回群、 f を群 H の元 x を群 G へ写す関数、 X_1, X_2 を群 G に値を持つ確率変数、確率変数 X_1 の実現値を x_1 、確率変数 X_2 の実現値を x_2 として、整数計算部が、互いに素である2つの自然数 a, b を用いて、

$a'a + b'b = 1$ の関係を満たす整数 a', b' を計算する。第一乱数化可能標本器は、 $f(x)^b x_1$ を計算可能であり、その計算結果を u とする。第一べき乗計算部は、 $u' = u^a$ を計算する。第二乱数化可能標本器は、 $f(x)^a x_2$ を計算可能であり、その計算結果を v とする。第二べき乗計算部は、 $v' = v^b$ を計算する。判定部は、 $u' = v'$ であるか判定する。最終計算部は、 $u' = v'$ であると判定された場合には、 $u^{b'}$ 、 $v^{a'}$ を計算する。

WO 2011/086992 A1



(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, 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：

代理計算システム、方法、依頼装置、プログラム及びその記録媒体

技術分野

[0001] この発明は、コンピュータによる計算技術に関する。特に、他の計算機に行わせた計算結果を用いて計算を行う技術に関する。

背景技術

[0002] 正しい計算をするとは限らない計算装置に依頼した計算の結果を用いて依頼装置が関数 f の計算を行う技術が、非特許文献 1 に記載されている。非特許文献 1 に記載された自己訂正器は、計算装置に計算を複数回依頼しその計算結果の多数決を採ることで関数 f の計算を行う（例えば、非特許文献 1 参照。）。

先行技術文献

非特許文献

[0003] 非特許文献 1：M. Blum, M. Luby, and R. Rubinfeld, “Self-Testing/Correcting with Applications to Numerical Problems”, STOC 1990, pp. 73-83.

発明の概要

発明が解決しようとする課題

[0004] しかしながら、非特許文献 1 の自己訂正器が正常に動作するためには、計算装置は一定以上の確率で正しい計算をする必要があり、正しい計算を行う確率が低い計算装置を用いて関数 f の計算をする技術は知られていないという課題がある。

課題を解決するための手段

[0005] この発明の第一の態様である代理計算システムは、 G 、 H を巡回群、 f を群 H の元 x を群 G へ写す関数、 X_1 、 X_2 を群 G に値を持つ確率変数、確率変

数 X_1 の実現値を x_1 、確率変数 X_2 の実現値を x_2 として、互いに素である2つの自然数 a, b を用いて、 $a' a + b' b = 1$ の関係を満たす整数 a', b' を計算する整数計算部と、 $f(x)^b x_1$ を計算可能であり、その計算結果を u とする第一乱数化可能標本器と、 $u' = u^a$ を計算する第一べき乗計算部と、 $f(x)^a x_2$ を計算可能であり、その計算結果を v とする第二乱数化可能標本器と、 $v' = v^b$ を計算する第二べき乗計算部と、 $u' = v'$ であるか判定する判定部と、 $u' = v'$ であると判定された場合には、 $u^{b'} v^{a'}$ を計算する最終計算部とを含む。

[0006] この発明の第二の態様である代理計算システムは、 G, H 及び F を巡回群とし、写像 $\theta: G \times H \rightarrow F$ を双同型準同型写像とし、 g を群 G の元とし、 h を群 H の元とし、 K_G を群 G の位数とし、 K_H を群 H の位数とし、 μ_g を群 G の生成元とし、 μ_h を群 H の生成元とし、 $\nu = \theta(\mu_g, \mu_h)$ とし、 k を自然数のセキュリティパラメータとし、 $K = 2^k$ として、依頼装置は、0以上 K_G 未満の整数の乱数 r_1 を生成する第一乱数生成部と、0以上 K_H 未満の整数の乱数 r_2 を生成する第二乱数生成部と、第一入力情報 $g_1 = \mu_g^{r_1} g$ を計算する第一入力情報計算部と、第二入力情報 $h_1 = \mu_h^{r_2}$ を計算する第二入力情報計算部と、計算装置から受信した $z_1 \in F$ を用いて、 $z_1 \nu^{-r_1 r_2}$ を計算する第一リスト情報計算部と、乱数 r_2 と計算された $z_1 \nu^{-r_1 r_2}$ とから構成される情報の組 $(r_2, z_1 \nu^{-r_1 r_2})$ が記憶される第一リスト記憶部と、0以上 K 未満の整数の一樣乱数である d_1 を生成する第三乱数生成部と、0以上 K_G 未満の整数の一樣乱数である r_4 を生成する第四乱数生成部と、0以上 K_H 未満の整数の一樣乱数である r_5 を生成する第五乱数生成部と、第三入力情報 $g_2 = \mu_g^{r_4} g^{d_1}$ を計算する第三入力情報計算部と、第四入力情報 $h_2 = \mu_h^{r_5}$ を計算する第四入力情報計算部と、計算装置から受信した $z_2 \in F$ を用いて、 $z_2 \nu^{-r_4 r_5}$ を計算する第二リスト情報計算部と、 d_1 と r_5 と計算された $z_2 \nu^{-r_4 r_5}$ とから構成される情報の組 $(d_1, r_5, z_2 \nu^{-r_4 r_5})$ が記憶される第二リスト記憶部と、第一リスト記憶部から読み込んだ情報の組の第一成分を s_1 とし、第二成分を w_1 とし、第二リスト記憶部から読み込んだ情報の組の第一

成分を t_2 とし、第二成分を s_2 とし、第三成分を w_2 として、これらの情報の組が $(w_1) \wedge (t_2 s_2 s_1^{-1}) = w_2$ の関係を満たすかを判定し、その関係を満たす場合には、 s_1 を σ に代入し、 w_1 を ν' に代入する第一判定部と、0 以上 K_G 未満の整数の一樣乱数である r_6 を生成する第六乱数生成部と、0 以上 K_H 未満の整数の一樣乱数である r_7 を生成する第七乱数生成部と、第五入力情報 $g_3 = g^{r_6}$ を計算する第五入力情報計算部と、第六入力情報 $h_3 = \mu_h^{r_7 \sigma h}$ を計算する第六入力情報計算部と、計算装置から受信した $z_3 \in F$ を用いて、 $z_3 \nu'^{-r_6 r_7}$ を計算する第三リスト情報計算部と、 r_6 と計算された $z_3 \nu'^{-r_6 r_7}$ とから構成される情報の組 $(r_6, z_3 \nu'^{-r_6 r_7})$ が記憶される第三リスト記憶部と、0 以上 K 未満の整数の一樣乱数である d_2 を生成する第八乱数生成部と、0 以上 K_G 未満の整数の一樣乱数である r_9 を生成する第九乱数生成部と、0 以上 K_H 未満の整数の一樣乱数である r_{10} を生成する第十乱数生成部と、第七入力情報 $g_4 = \mu_g^{r_9}$ を計算する第七入力情報計算部と、第八入力情報 $h_4 = \mu_h^{r_{10} \sigma h^{d_2}}$ を計算する第八入力情報計算部と、計算装置から受信した $z_4 \in F$ を用いて、 $z_4 \nu'^{-r_9 r_{10}}$ を計算する第四リスト情報計算部と、 d_2 と r_9 と計算された $z_4 \nu'^{-r_9 r_{10}}$ とから構成される情報の組 $(d_2, r_9, z_4 \nu'^{-r_9 r_{10}})$ が記憶される第四リスト記憶部と、第三リスト記憶部から読み込んだ情報の組の第一成分を s_3 とし、第二成分を w_3 とし、第四リスト記憶部から読み込んだ情報の組の第一成分を t_4 とし、第二成分を s_4 とし、第三成分を w_4 として、これらの情報の組が $(w_3) \wedge (t_4 s_4 s_3^{-1}) = w_4$ の関係を満たすかを判定し、その関係を満たす場合には、 $(w_3) \wedge (s_3^{-1})$ を出力する第二判定部と、を含む。計算装置は、依頼装置から受信した g_1 及び h_1 を用いて $\theta(g_1, h_1)$ を計算可能であり、その計算結果を z_1 として出力する第一出力情報計算部と、依頼装置から受信した g_2 及び h_2 を用いて $\theta(g_2, h_2)$ を計算可能であり、その計算結果を z_2 として出力する第二出力情報計算部と、依頼装置から受信した g_3 及び h_3 を用いて $\theta(g_3, h_3)$ を計算可能であり、その計算結果を z_3 として出力する第三出力情報計算部と、依頼装置から受信した g_4 及び h_4 を用いて $\theta(g_4, h_4)$ を

計算可能であり、その計算結果を z_4 として出力する第四出力情報計算部とを含む。

発明の効果

[0007] 正しい計算を行う確率が低い計算装置を用いて関数 f の計算をすることができる。

図面の簡単な説明

[0008] [図1] 第一実施形態から第三実施形態の代理計算システムの例の機能ブロック図。

[図2] 第一実施形態から第三実施形態の依頼装置及び計算装置の例の機能ブロック図。

[図3] 第一実施形態から第三実施形態の標本器の例の機能ブロック図。

[図4] 第一実施形態から第三実施形態の第一乱数化可能標本器及び第二乱数化可能標本器の例の機能ブロック図。

[図5] 第一実施形態から第三実施形態の第一乱数化可能標本器及び第二乱数化可能標本器の他の例の機能ブロック図。

[図6] 第一実施形態から第三実施形態の代理計算方法の例の流れ図。

[図7] ステップ S 3 の例を示す流れ図。

[図8] ステップ S 6 の例を示す流れ図。

[図9] ステップ S 3 の他の例を示す流れ図。

[図10] ステップ S 6 の他の例を示す流れ図。

[図11] 第四実施形態から第十実施形態の代理計算システムの例の機能ブロック図。

[図12] 第四実施形態から第十実施形態の依頼装置の例の機能ブロック図。

[図13] 第四実施形態から第十実施形態の依頼装置の例の機能ブロック図。

[図14] 第四実施形態から第十実施形態の計算装置の例の機能ブロック図。

[図15] 第四実施形態から第十実施形態の代理計算方法の例の流れ図。

[図16] 第四実施形態から第十実施形態の代理計算方法の例の流れ図。

[図17] 代理計算システムの変形例の機能ブロック図。

発明を実施するための形態

[0009] 以下、この発明による代理計算システム、代理計算方法の実施形態を詳細に説明する。

第一実施形態から第二実施形態は、依頼装置 1 が計算装置 2 に依頼した計算の結果を用いて $f(x)$ を計算するものである。

[0010] [第一実施形態]

第一実施形態の代理計算システムは、図 1 に例示するように依頼装置 1 及び計算装置 2 を含み、依頼装置 1 が計算装置 2 に依頼した計算の結果を用いて $f(x)$ を計算する。

[0011] 依頼装置 1 は、図 2 に示すように、自然数記憶部 11、整数計算部 12、第一べき乗計算部 13、第一リスト記憶部 14、判定部 15、第二べき乗計算部 16、第二リスト記憶部 17、制御部 18 及び最終計算部 19 を例えば含む。計算装置 2 は、第一乱数化可能標本器 21 及び第二乱数化可能標本器 22 を例えば含む。第一実施形態においては、第一乱数化可能標本器 21 及び第二乱数化可能標本器 22 が計算装置 2 に対応する。

[0012] G, H を巡回群、関数 $f: H \rightarrow G$ を群 H の元 x を群 G へ写す関数、群 G, H の生成元をそれぞれ μ_g, μ_h, X_1, X_2 を群 G に値を持つ確率変数、確率変数 X_1 の実現値を x_1 、確率変数 X_2 の実現値を x_2 とする。

[0013] 自然数記憶部 11 には、互いに素である 2 つの自然数 a, b の組 (a, b) が複数記憶されているものとする。 I を群 G の位数未満の 2 つの自然数の組で互いに素なもの集合とすると、自然数記憶部 11 には I の部分集合 S に対応する自然数 a, b の組 (a, b) が記憶されていると考えることができる。

[0014] 整数計算部 12 は、自然数記憶部 11 に記憶された複数の自然数の組 (a, b) から、1 つの自然数の組 (a, b) をランダムに読み込み、その読み込んだ自然数の組 (a, b) を用いて、 $a' a + b' b = 1$ の関係を満たす整数 a', b' を計算する（ステップ S1）。自然数 a, b は互いに素であるため、 $a' a + b' b = 1$ の関係を満たす整数 a', b' は必ず存在する

。自然数の組 (a, b) についての情報は、第一べき乗計算部 13、第二べき乗計算部 16、第一乱数化可能標本器 21 及び第二乱数化可能標本器 22 に送られる。自然数の組 (a', b') についての情報は、最終計算部 19 に送られる。

[0015] 制御部 18 は、 $t = 1$ とする（ステップ S2）。

第一乱数化可能標本器 21 は、 $f(x)^b x_1$ を計算可能であり、 x 及び b を用いて計算を行い、その計算結果を u とする（ステップ S3）。計算結果 u は、第一べき乗計算部 13 に送られる。

[0016] この出願において、計算可能とは、無視することができない確率以上の確率で計算することができることを意味する。無視することができない確率とは、セキュリティパラメータ k についての広義単調関数である多項式を多項式 $F(k)$ として、 $1/F(k)$ 以上の確率である。

[0017] ここで、 $f(x)^b x_1$ を計算するとは、 $f(x)^b x_1$ と定義される式の値を計算することである。式 $f(x)^b x_1$ の値を最終的に計算することができれば、途中の計算方法は問わない。これは、この出願で登場する他の式の計算についても同様である。

[0018] 第一べき乗計算部 13 は、 $u' = u^a$ を計算する（ステップ S4）。計算結果 u とその計算結果に基づいて計算された u' との組 (u, u') は、第一リスト記憶部 14 に記憶される。

[0019] 判定部 15 は、第一リスト記憶部 14 に記憶された組 (u, u') 及び第二リスト記憶部 17 に記憶された組 (v, v') の中で、 $u' = v'$ となるものがあるか判定する（ステップ S5）。もし、第二リスト記憶部 17 に組 (v, v') が記憶されていない場合には、このステップ S5 の処理を行わずに、次のステップ S6 の処理を行う。 $u' = v'$ となるものがあつた場合には、ステップ 12 に進む。 $u' = v'$ となるものがなかった場合には、ステップ S6 に進む。

[0020] 第二乱数化可能標本器 22 は、 $f(x)^a x_2$ を計算可能であり、 x 及び a を用いて計算を行い、その計算結果を v とする（ステップ S6）。計算結果

v は、第二べき乗計算部 16 に送られる。

[0021] 第二べき乗計算部 16 は、 $v' = v^b$ を計算する（ステップ S 7）。計算結果 v とその計算結果に基づいて計算された v' との組 (v, v') は、第二リスト記憶部 17 に記憶される。

[0022] 判定部 15 は、第一リスト記憶部 14 に記憶された組 (u, u') 及び第二リスト記憶部 17 に記憶された組 (v, v') の中で、 $u' = v'$ となるものがあるか判定する（ステップ S 8）。 $u' = v'$ となるものがあつた場合には、ステップ 12 に進む。 $u' = v'$ となるものがなかった場合には、ステップ S 9 に進む。

[0023] 制御部 18 は、 $t = T$ であるか判定する（ステップ S 9）。 T は予め定められた自然数である。 $t = T$ であれば、計算をすることができなかった旨の情報、例えば記号「 $\perp$ 」を出力して（ステップ S 11）、処理を終える。 $t = T$ でない場合には、制御部 18 は、 t を 1 だけインクリメント、すなわち $t = t + 1$ として（ステップ S 10）、ステップ S 3 に戻る。

[0024] 計算をすることができなかった旨の情報（この例では記号「 $\perp$ 」）は、計算装置 2 が正しく計算を行う信頼性が T で定められる基準を下回るということを意味する。言い換えれば、 T 回の繰り返しで正しい演算を行うことができなかったということの意味する。

[0025] 最終計算部 19 は、 $u' = v'$ であると判定された場合には、その u' 及び v' に対応する u 及び v を用いて $u^{b'} v^{a'}$ を計算して、出力する（ステップ S 12）。計算された $u^{b'} v^{a'} = f(x)$ となる。 $u^{b'} v^{a'} = f(x)$ となる理由については、後述する。

[0026] ≪ $u^{b'} v^{a'} = f(x)$ となる理由について ≫

X を群 G に値を持つ確率変数とする。 $w \in G$ について、ある計算装置で要求を受けるたびに確率変数 R に従って標本 x' を抽出し $w x'$ を返信するものを、 w について誤差 X を持つ標本器 (sampler) と呼ぶ。

[0027] $w \in G$ について、ある計算装置で自然数 a の入力を受けるたびに確率変数 X に従って標本 x' を抽出し $w^a x'$ を返信するものを、 w について誤差 X を

持つ乱数化可能標本器 (randomizable sampler) と呼ぶ。乱数化可能標本器は $a = 1$ として用いられれば標本器として機能する。

[0028] 上記実施形態の代理計算システムは、 x を入力として $f(x)$ を出力する代理計算システムを構成するに当たり、 $f(x)$ について誤差 X_1 を持つ第一乱数化可能標本器 21、 $f(x)$ について誤差 X_2 を持つ第二乱数化可能標本器 22 を用いている。

[0029] $u' = v'$ が成立するのは、すなわち $u^a = v^b$ が成立するのは、第一乱数化可能標本器 21 が $u = f(x)^b x_1$ を正しく計算しており、第二乱数化可能標本器 22 が $v = f(x)^a x_2$ を正しく計算しており、さらに x_1 及び x_2 が群 G の単位元 e_g である可能性が非常に高いことを発明者は見出した。ここでは、その証明は省略する。

[0030] 第一乱数化可能標本器 21 が $u = f(x)^b x_1$ を正しく計算しており、第二乱数化可能標本器 22 が $v = f(x)^a x_2$ を正しく計算しており、 x_1 及び x_2 が群 G の単位元 e_g であるとき、 $u^{b'} v^{a'} = (f(x)^b x_1)^{b'} (f(x)^a x_2)^{a'} = (f(x)^b e_g)^{b'} (f(x)^a e_g)^{a'} = f(x)^{b b'} e_g^{b'} f(x)^{a a'} e_g^{a'} = f(x)^{(b b' + a a')} = f(x)$ となる。

[0031] $(q_1, q_2) \in I$ について、 $i = 1, 2$ の各々について関数 π_i を $\pi_i(q_1, q_2) = q_i$ で定義する。また、 $L = \min(\#\pi_1(S), \#\pi_2(S))$ とする。 $\# \cdot$ は、集合 $\cdot$ の位数である。群 G が巡回群や位数の計算が困難な群であるときには、上記代理計算システムが「 $\perp$ 」以外を出力するときの出力が $f(x)$ ではない確率は、無視できる程度の誤差の範囲で高々 $T^2 L / \#S$ 程度と期待することができる。もし $L / \#S$ が無視できる量で T が多項式オーダー程度の量であれば、上記代理計算システムは圧倒的な確率で $f(x)$ を出力する。

$L / \#S$ が無視できる量になるような S の例には、例えば $S = \{(1, d) \mid d \in [2, |G| - 1]\}$ がある。

[0032] なお、図 2 に破線で示すように、計算装置 2 に標本器 23 を設けてもよい。標本器 23 は、 X_3 を群 G に値を持つ確率変数、確率変数 X_3 の実現値を x_3

として、 $f(x) \times v$ を計算可能であり、 $a = 1$ あれば第二乱数化可能標本器 22 に代わりその計算結果を上記 v とし、 $b = 1$ であれば第一乱数化可能標本器 21 に代わりその計算結果を上記 u とする。

[0033] 一般に乱数化可能標本器よりも標本器の計算量は小さい。 $a = 1$ 、 $b = 1$ のときに第一乱数化可能標本器 21、第二乱数化可能標本器 22 に代わり、標本器 23 が計算を行うことで、計算装置 2 の計算量を小さくすることができる。

[0034] [第二実施形態]

第二実施形態の代理計算システムは、第一乱数化可能標本器 21 及び第二乱数化可能標本器 22 の一例、言い換えればステップ S3 及びステップ S6 の一例を具体化したものである。以下、第一実施形態と異なる部分を中心に説明し、共通する部分については重複説明を省略する。

[0035] 第二実施形態の第一乱数化可能標本器 21 は、図 3 に示すように、第一乱数生成部 110、第一入力情報計算部 111、第一出力情報計算部 24 及び第一計算部 112 を例えば含む。また、第二実施形態の第二乱数化可能標本器 22 は、図 3 に示すように、第二乱数生成部 113、第二入力情報計算部 114、第二出力情報計算部 25 及び第二計算部 115 を例えば含む。

[0036] 第二実施形態においては、第一乱数生成部 110、第一入力情報計算部 111、第一計算部 112、第二乱数生成部 113、第二入力情報計算部 114 及び第二計算部 115 は、依頼装置 1 に含まれる。また、第一出力情報計算部 24 及び第二出力情報計算部 25 は、計算装置 2 に含まれる。第二実施形態においては、第一出力情報計算部 24 及び第二出力情報計算部 25 が計算装置 2 に対応する。

[0037] 第二実施形態の関数 f は準同型写像であるとする。また、群 H の生成元を μ_h 、群 H の位数を K_H 、 $v = f(\mu_h)$ とする。

[0038] ステップ S3 は、図 7 に例示するステップ S31 からステップ S34 で構成される。

[0039] 第一乱数生成部 110 は、0 以上 K_H 未満の整数の一樣乱数 r_1 を生成する

(ステップS 3 1)。生成された乱数 r_1 は、第一入力情報計算部 1 1 1 に送られる。

第一入力情報計算部 1 1 1 は、第一入力情報 $\mu_{h r_1} x^b$ を計算する (ステップS 3 2)。計算された第一入力情報 $\mu_{h r_1} x^b$ は、第一出力情報計算部 2 4 に送られる。

第一出力情報計算部 2 4 は、第一入力情報 $\mu_{h r_1} x^b$ を用いて計算を行い、その計算結果を第一出力情報 z_1 とする (ステップS 3 3)。計算された第一出力情報 z_1 は、第一計算部 1 1 2 に送られる。

第一出力情報計算部 2 4 は、 $f(\mu_{h r_1} x^b)$ を計算可能である。第一出力情報計算部 2 4 による計算の結果が $f(\mu_{h r_1} x^b)$ であることもあれば、 $f(\mu_{h r_1} x^b)$ でないこともある。

[0040] ここで、 μ_h の右肩の r_1 は、 r_1 のことである。このように、この出願において、 α を第一の文字、 β を第二の文字、 γ を数字として、 $\alpha^{\beta\gamma}$ と表記した場合には、その $\beta\gamma$ は β_γ 、すなわち β の下付き γ を意味する。

第一計算部 1 1 2 は、 $z_1 \nu^{-r_1}$ を計算してその計算結果を u とする (ステップS 3 4)。計算結果 u は、第一べき乗計算部 1 3 に送られる。ここで、 $u = z_1 \nu^{-r_1} = f(x)^b x_1$ となる。すなわち、 $z_1 \nu^{-r_1}$ は、 $f(x)$ について誤差 x_1 を持つ乱数化可能標本器となる。その理由については後述する。

[0041] ステップS 6 は、図 8 に例示するステップS 6 1 からステップS 6 4 で構成される。

[0042] 第二乱数生成部 1 1 3 は、0 以上 K_H 未満の整数の一樣乱数 r_2 を生成する (ステップS 6 1)。生成された乱数 r_2 は、第二入力情報計算部 1 1 4 に送られる。

第二入力情報計算部 1 1 4 は、第二入力情報 $\mu_{h r_2} x^a$ を計算する (ステップS 6 2)。計算された第二入力情報 $\mu_{h r_2} x^a$ は、第二出力情報計算部 2 5 に送られる。

第二出力情報計算部 2 5 は、第二入力情報 $\mu_{h r_2} x^a$ を用いて計算を行い、その計算結果を第二出力情報 z_2 とする (ステップS 6 3)。計算された第二

出力情報 z_2 は、第二計算部 115 に送られる。

- [0043] 第二出力情報計算部 25 は、 $f(\mu_{h^{r^2}} x^a)$ を計算可能である。第二出力情報計算部 25 による計算の結果が $f(\mu_{h^{r^2}} x^a)$ であることもあれば、 $f(\mu_{h^{r^2}} x^a)$ でないこともある。

第二計算部 115 は、 $z_2 \nu^{-r^2}$ を計算してその計算結果を v とする（ステップ S64）。計算結果 v は、第二べき乗計算部 16 に送られる。ここで、 $v = z_2 \nu^{-r^2} = f(x)^a x_2$ となる。すなわち、 $z_2 \nu^{-r^2}$ は、 $f(x)$ について誤差 x_2 を持つ乱数化可能標本器となる。その理由については後述する。

- [0044] 第二実施形態においても、 $a = 1$ 、 $b = 1$ のときは、第一乱数化可能標本器 21 又は第二乱数化可能標本器 22 に代わり、標本器 23 が u 又は v の値を計算することにより、計算量を削減してもよい。

- [0045] 第二実施形態の標本器 23 は、図 4 に示すように、第三乱数生成部 116、第三入力情報計算部 117、第三出力情報計算部 26、第三計算部 118 を例えば含む。第三乱数生成部 116、第三入力情報計算部 117 及び第三計算部 118 は依頼装置 1 に含まれる。第三出力情報計算部 26 は計算装置 2 に含まれる。

- [0046] $a = 1$ 、 $b = 1$ であれば、第一乱数化可能標本器 21、第二乱数化可能標本器 22 に代わり標本器 23 の各部は以下の処理を行う。

第三乱数生成部 116 は、0 以上 K_H 未満の整数の乱数 r_3 を生成する。生成された乱数 r_3 は第三入力情報計算部 117 に送られる。

第三入力情報計算部 117 は、第三入力情報 x^{r_3} を計算する。計算された第三入力情報 x^{r_3} は、第三出力情報計算部 26 に送られる。

- [0047] 第三出力情報計算部 26 は、第三入力情報 x^{r_3} を用いて計算を行い、その計算結果を第三出力情報 z_3 とする。計算された第三出力情報 z_3 は、第三計算部 118 に送られる。

第三出力情報計算部 26 は、 $f(x^{r_3})$ を計算可能である。第三出力情報計算部 26 による計算の結果が $f(x^{r_3})$ であることもあれば、 $f(x^{r_3})$ でないこともある。

[0048] 第三計算部 118 は、 z_3^{1/r^3} を計算してその計算結果を、 $a = 1$ であれば v とし、 $b = 1$ であれば u とする。計算結果 v は第二べき乗計算部 16 に送られる。計算結果 u は第一べき乗計算部 13 に送られる。ここで、 $u = v = z_3^{1/r^3} = f(x) \times x_3$ となる。すなわち、 z_3^{1/r^3} は、 $f(x)$ について誤差 X_3 を持つ標本器となる。 z_3^{1/r^3} は、 $f(x)$ について誤差 X_3 を持つ標本器となる。その理由については後述する。

[0049] z_3^{1/r^3} の計算、すなわち z_3 のべき乗根の計算が困難な場合には、次のようにして u 及び v を計算してもよい。第三計算部 118 は、乱数 r_3 とその乱数 r_3 に基づいて計算された z_3 の組を順次 (α_1, β_1) , (α_2, β_2) , $\dots$, (α_m, β_m) , $\dots$ として図示していない記憶部に記憶する。 m は自然数である。第三計算部 118 は、 $\alpha_1, \alpha_2, \dots, \alpha_m$ の最小公倍数が 1 になれば、 $\gamma_1, \gamma_2, \dots, \gamma_m$ を整数として $\gamma_1 \alpha_1 + \gamma_2 \alpha_2 + \dots + \gamma_m \alpha_m = 1$ となる $\gamma_1, \gamma_2, \dots, \gamma_m$ を計算して、その $\gamma_1, \gamma_2, \dots, \gamma_m$ を用いて $\prod_{i=1}^m \beta_i^{r_i} = \beta_1^{\gamma_1} \beta_2^{\gamma_2} \dots \beta_m^{\gamma_m}$ を計算して、その計算結果を u 及び v としてもよい。

[0050] このように、乱数 r_1, r_2, r_3 を用いて x を攪乱した情報を計算装置 2 に送ることにより、関数 f の値の計算の対象となる $x \in H$ を依頼装置 1 と計算装置 2 との間の通信を傍受する第三者、及び、計算装置 2 に対して秘匿化することができる。

[0051] ≪ $z_1 \nu^{-r^1}, z_2 \nu^{-r^2}$ が $f(x)$ についてそれぞれ誤差 X_1, X_2 を持つ乱数化可能標本器となる理由について ≫

c を自然数、 R 及び R' を乱数として、計算装置 2 が $\mu_h^R x^c$ を用いて行う計算の計算結果を $B(\mu_h^R x^c)$ (すなわち、計算装置 2 が依頼装置 1 に返す計算結果を z とすると、 $z = B(\mu_h^R x^c)$ である。) とし、群 G に値を持つ確率変数 X を $X = B(\mu_h^{R'}) f(\mu_h^{R'})^{-1}$ と定義する。

[0052] このとき、 $z \nu^{-R} = B(\mu_h^R x^c) f(\mu_h)^{-R} = X f(\mu_h^R x^c) f(\mu_h)^{-R} = X f(\mu_h)^R f(x)^c f(\mu_h)^{-R} = f(x)^c X$ となる。すなわち、 $z \nu^{-R}$ は、 $f(x)$ について誤差 X を持つ乱数化可能標本器となる。

[0053] 上記式展開において、 $X = B(\mu_h^{R'}) f(\mu_h^{R'})^{-1} = B(\mu_h^R x^c) f(\mu_h^R x^c)^{-1}$ であり、 $B(\mu_h^R x^c) = X f(\mu_h^R x^c)$ であるという性質を用いている。この性質は、関数 f が準同型写像であり、 R 及び R' が乱数であることに基づく。

[0054] したがって、 a, b が自然数、 r_1, r_2 が乱数であることを考慮すると、同様に、 $z_1 \nu^{-r_1}, z_2 \nu^{-r_2}$ が $f(x)$ についてそれぞれ誤差 X_1, X_2 を持つ乱数化可能標本器となるのである。

[0055] ≪ z_3^{1/r_3} が $f(x)$ について誤差 X_3 を持つ標本器となる理由について≫
 R 及び R' を乱数として、計算装置 2 が x^R を用いて行う計算の計算結果を $B(x^R)$ (すなわち、計算装置 2 が依頼装置 1 に返す計算結果を z とすると、 $z = B(x^R)$ である。) とし、群 G に値を持つ確率変数 X を $X = B(x^R)^{1/R} f(x)^{-1}$ と定義する。

このとき、 $z^{1/R} = B(x^R)^{1/R} = X f(x) = f(x) X$ となる。すなわち、 $z^{1/R}$ は、 $f(x)$ について誤差 X を持つ標本器となる。

[0056] 上記式展開において、 $X = B(x^R)^{1/R} f(x^R)^{-1}$ であり、 $B(x^R)^{1/R} = X f(x^R)$ であるという性質を用いている。この性質は、 R 及び R' が乱数であることに基づく。

したがって、 r_3 が乱数であることを考慮すると、 $z^{1/R}$ が $f(x)$ について誤差 X_3 を持つ乱数化可能標本器となるのである。

[0057] [第三実施形態]

第三実施形態の代理計算システムは、第一乱数化可能標本器 2 1 及び第二乱数化可能標本器 2 2 の他の例、言い換えればステップ S 3 及びステップ S 6 の他の例を具体化したものである。具体的には、 $H = G \times G$ で、関数 f が $E | G a m a |$ 暗号の復号関数、すなわち秘密鍵 s 及び暗号文 (c_1, c_2) に対して $f(c_1, c_2) = c_1 c_2^{-s}$ である場合の第一乱数化可能標本器 2 1 及び第二乱数化可能標本器 2 2 の例を具体化したものである。以下、第一実施形態と異なる部分を中心に説明し、共通する部分については重複説明を省略する。

[0058] 第三実施形態の第一乱数化可能標本器 2 1 は、図 5 に示すように、第四乱数生成部 1 1 9、第五乱数生成部 1 2 0、第四入力情報計算部 1 2 1、第五入力情報計算部 1 2 2、第四出力情報計算部 2 7 及び第四計算部 1 2 3 を例えば含む。第二乱数化可能標本器 2 2 は、図 5 に示すように、第六乱数生成部 1 2 4、第七乱数生成部 1 2 5、第六入力情報計算部 1 2 6、第七入力情報計算部 1 2 7、第五出力情報計算部 2 8 及び第五計算部 1 2 8 を例えば含む。

[0059] 第四乱数生成部 1 1 9、第五乱数生成部 1 2 0、第四入力情報計算部 1 2 1、第五入力情報計算部 1 2 2、第四計算部 1 2 3、第六乱数生成部 1 2 4、第七乱数生成部 1 2 5、第六入力情報計算部 1 2 6、第七入力情報計算部 1 2 7、第五出力情報計算部 2 8 及び第五計算部 1 2 8 は、依頼装置 1 に含まれる。第四出力情報計算部 2 7 及び第五出力情報計算部 2 8 は計算装置 2 に含まれる。第三実施形態では、第四出力情報計算部 2 7 及び第五出力情報計算部 2 8 が計算装置 2 に対応する。

[0060] 第三実施形態では、 $x = (c_1, c_2)$ であり、 $f(c_1, c_2)$ は直積群 $G \times G$ から G への準同型写像であり、群 G の生成元を μ_g とし、群 G の位数を K_g とし、同じ秘密鍵 s に対する暗号文 $(V, W) \in H$ とその暗号文を復号した復号文 $f(V, W) = Y \in G$ とを依頼装置 1 と計算装置 2 は事前に知っているとする。

[0061] 第三実施形態のステップ S 3 は、図 9 に例示するステップ S 3 1' からステップ S 3 6' で構成される。

[0062] 第四乱数生成部 1 1 9 は、0 以上 K_g 未満の整数の一樣乱数 r_4 を生成する（ステップ S 3 1'）。生成された乱数 r_4 は、第四入力情報計算部 1 2 1、第五入力情報計算部 1 2 2 及び第四計算部 1 2 3 に送られる。

第五乱数生成部 1 2 0 は、0 以上 K_g 未満の整数の一樣乱数 r_5 を生成する（ステップ S 3 2'）。生成された乱数 r_5 は、第四入力情報計算部 1 2 1 及び第四計算部 1 2 3 に送られる。

[0063] 第四入力情報計算部 1 2 1 は、第四入力情報 $c_1^b V^{r_4} \mu_g^{r_5}$ を計算する（

ステップS 3 3')。計算された第四入力情報 $c_1^b V^{r^4} \mu_g^{r^5}$ は、第四出力情報計算部 2 7 に送られる。

第五入力情報計算部 1 2 2 は、第五入力情報 $c_2^b W^{r^4}$ を計算する（ステップS 3 4')。計算された第五入力情報 $c_2^b W^{r^4}$ は、第四出力情報計算部 2 7 に送られる。

[0064] 第四出力情報計算部 2 7 は、第四入力情報 $c_1^b V^{r^4} \mu_g^{r^5}$ 及び第五入力情報 $c_2^b W^{r^4}$ を用いて計算を行い、その計算結果を第四出力情報 z_4 とする（ステップS 3 5')。

第四出力情報計算部 2 7 は、 $f(c_1^b V^{r^4} \mu_g^{r^5}, c_2^b W^{r^4})$ を計算可能である。第四出力情報計算部 2 7 による計算の結果が $f(c_1^b V^{r^4} \mu_g^{r^5}, c_2^b W^{r^4})$ であることもあれば、 $f(c_1^b V^{r^4} \mu_g^{r^5}, c_2^b W^{r^4})$ でないこともある。

[0065] 第四計算部 1 2 3 は、 $z_4 Y^{-r^4} \mu_g^{-r^5}$ を計算してその計算結果を u とする（ステップS 3 6')。計算結果 u は、第一べき乗計算部 1 3 に送られる。ここで、 $u = z_4 Y^{-r^4} \mu_g^{-r^5} = f(c_1, c_2)^b x_1$ となる。すなわち、 $z_4 Y^{-r^4} \mu_g^{-r^5}$ は、 $f(c_1, c_2)$ について誤差 X_1 を持つ乱数化可能標本器となる。その理由については後述する。

[0066] 第三実施形態のステップS 6 は、図 1 0 に例示するステップS 6 1' からステップS 6 6' で構成される。

[0067] 第六乱数生成部 1 2 4 は、0 以上 K_g 未満の整数の一樣乱数 r_6 を生成する（ステップS 6 1')。生成された乱数 r_6 は、第六入力情報計算部 1 2 6、第七入力情報計算部 1 2 7 及び第五計算部 1 2 8 に送られる。

第七乱数生成部 1 2 5 は、0 以上 K_g 未満の整数の一樣乱数 r_7 を生成する（ステップS 6 2')。生成された乱数 r_7 は、第六入力情報計算部 1 2 6 及び第五計算部 1 2 8 に送られる。

[0068] 第六入力情報計算部 1 2 6 は、第六入力情報 $c_1^a V^{r^6} \mu_g^{r^7}$ を計算する（ステップS 6 3')。計算された第六入力情報 $c_1^a V^{r^6} \mu_g^{r^7}$ は、第五出力情報計算部 2 8 に送られる。

第七入力情報計算部 127 は、第七入力情報 $c_2^a W^{r6}$ を計算する（ステップ S64'）。計算された第七入力情報 $c_2^a W^{r6}$ は、第五出力情報計算部 28 に送られる。

[0069] 第五出力情報計算部 28 は、上記第六入力情報 $c_1^a V^{r6} \mu_g^{r7}$ 及び上記第七入力情報 $c_2^a W^{r6}$ を用いて計算を行い、その計算結果を第五出力情報 z_5 とする（ステップ S65'）。計算された第五出力情報 z_5 は、第五計算部 128 に送られる。

第五出力情報計算部 28 は、 $f(c_1^a V^{r6} \mu_g^{r7}, c_2^a W^{r6})$ を計算可能である。第五出力情報計算部 28 による計算の結果が $f(c_1^a V^{r6} \mu_g^{r7}, c_2^a W^{r6})$ であることもあれば、 $f(c_1^a V^{r6} \mu_g^{r7}, c_2^a W^{r6})$ でないこともある。

[0070] 第五計算部 128 は、 $z_5 Y^{-r6} \mu_g^{-r7}$ を計算してその計算結果を v とする（ステップ S66'）。計算結果 v は、第二べき乗計算部 16 に送られる。ここで、 $v = z_5 Y^{-r6} \mu_g^{-r7} = f(c_1, c_2)^a x_2$ となる。すなわち、 $z_5 Y^{-r6} \mu_g^{-r7}$ は、 $f(c_1, c_2)$ について誤差 x_2 を持つ乱数化可能標本器となる。その理由については後述する。

[0071] $\ll z_4 Y^{-r4} \mu_g^{-r5}, z_5 Y^{-r6} \mu_g^{-r7}$ が $f(c_1, c_2)$ についてそれぞれ誤差 x_1, x_2 を持つ乱数化可能標本器となる理由について

c を自然数、 R_1, R_2, R_1' 及び R_2' を乱数として、計算装置 2 が $c_1^c V^{R1} \mu_g^{R2}$ 及び $c_2^c W^{R1}$ を用いて行う計算の計算結果を $B(c_1^c V^{R1} \mu_g^{R2}, c_2^c W^{R1})$ （すなわち、計算装置 2 が依頼装置 1 に返す計算結果を z とすると、 $z = B(c_1^c V^{R1} \mu_g^{R2}, c_2^c W^{R1})$ である。）とし、群 G に値を持つ確率変数 X を $X = B(V^{R1'} \mu_g^{R2'}, W^{R1'}) f(V^{R1'} \mu_g^{R2'}, W^{R1'})^{-1}$ と定義する。

[0072] このとき、 $z Y^{-R1} \mu_g^{-R2} = B(c_1^c V^{R1} \mu_g^{R2}, c_2^c W^{R1}) Y^{-R1} \mu_g^{-R2} = X f(c_1^c V^{R1} \mu_g^{R2}, c_2^c W^{R1}) Y^{-R1} \mu_g^{-R2} = X f(c_1, c_2)^c f(V, W)^{R1} f(\mu_g, e_g)^{R2} Y^{-R1} \mu_g^{-R2} = X f(c_1, c_2)^c Y^{R1} \mu_g^{R2} Y^{-R1} \mu_g^{-R2} = f(c_1, c_2)^c X$ となる。すなわち、 $z Y^{-R1} \mu_g^{-R2}$ は

、 $f(x)$ について誤差 X を持つ乱数化可能標本器となる。なお、 e_g は、群 G の単位元である。

[0073] 上記式展開において、 $X = B(V^{R1'} \mu_g^{R2'}, W^{R1'}) f(V^{R1'} \mu_g^{R2'}, W^{R1'})^{-1} = B(c_1^c V^{R1} \mu_g^{R2}, c_2^c W^{R1}) f(c_1^c V^{R1} \mu_g^{R2}, c_2^c W^{R1})$ であり、 $B(c_1^c V^{R1} \mu_g^{R2}, c_2^c W^{R1}) = X f(c_1^c V^{R1} \mu_g^{R2}, c_2^c W^{R1})$ であるという性質を用いている。この性質は、 R_1 、 R_2 、 R_1' 及び R_2' が乱数であることに基づく。

[0074] したがって、 a 、 b が自然数、 r_4 、 r_5 、 r_6 及び r_7 が乱数であることを考慮すると、同様に、 $z_4 Y^{-r_4} \mu_g^{-r_5}$ 、 $z_5 Y^{-r_6} \mu_g^{-r_7}$ が $f(c_1, c_2)$ についてそれぞれ誤差 X_1 、 X_2 を持つ乱数化可能標本器となるのである。

[0075] [第一実施形態から第三実施形態の変形例等]

確率変数 X_1 、 X_2 及び X_3 は、同じでも異なってもよい。

第一乱数生成部 110、第二乱数生成部 113、第三乱数生成部 116、第四乱数生成部 119、第五乱数生成部 120、第六乱数生成部 124 及び第七乱数生成部 125 のそれぞれは、一様乱数を生成することにより、代理計算システムの安全性が最も高くなる。しかし、求める安全性のレベルがそれほど高くない場合には、第一乱数生成部 110、第二乱数生成部 113、第三乱数生成部 116、第四乱数生成部 119、第五乱数生成部 120、第六乱数生成部 124 及び第七乱数生成部 125 のそれぞれは、一様乱数ではない乱数を生成してもよい。

[0076] 上記の例では、第一乱数化可能標本器 21、第二乱数化可能標本器 22 を一回づつ呼び出しているが、依頼装置 1 と計算装置 2 との間の通信回数を減らすために、同一の a 、 b に対して第一乱数化可能標本器 21、第二乱数化可能標本器 22 を複数回呼び出して、依頼装置 1 が一回の通信で複数の u 、 v を取得できるようにしてもよい。

[0077] 第一乱数化可能標本器 21、第二乱数化可能標本器 22 及び標本器 23 の各部は、依頼装置 1 に配置してもよいし、計算装置 2 に配置してもよい。すなわち、第一実施形態のように各部のすべてを計算装置 2 に配置してもよい。

し、例えば第二実施形態及び第三実施形態のように依頼装置 1 及び計算装置 2 に分けて配置してもよい。

[0078] 依頼装置 1 の各部間のデータのやり取りは直接行われてもよいし、図示していない記憶部を介して行われてもよい。同様に、計算装置 2 の各部間のデータのやり取りは直接行われてもよいし、図示していない記憶部を介して行われてもよい。

[0079] 依頼装置 1 及び計算装置 2 のそれぞれはコンピュータによって実現することができる。この場合、この装置が有すべき各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、これ装置における各処理機能が、コンピュータ上で実現される。

[0080] 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。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、これらの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。

[0081] [第四実施形態]

第四実施形態から第十実施形態は、依頼装置 1' が計算装置 2' に依頼した計算の結果を用いて $\theta(g, h)$ を計算するものである。

[0082] 第四実施形態の代理計算システムは、図 11 に例示するように依頼装置 1' 及び計算装置 2' を含み、依頼装置 1' が計算装置 2' に依頼した計算の結果を用いて双準同型写像 $\theta(g, h)$ を計算する。

[0083] ここで、 G 、 H 及び F を巡回群とし、写像 $\theta : G \times H \rightarrow F$ を双準同型写像とし、 g を群 G の元とし、 h を群 H の元とし、 K_G を群 G の位数とし、 K_H を群 H の位数とし、 μ_g を群 G の生成元とし、 μ_h を群 H の生成元とし、 $\nu = \theta(\mu_g, \mu_g)$ とし、 k を 1 以上の整数のセキュリティパラメータとし、 $K = 2^k$ とする。

[0084] 双準同型写像とは、2 つの入力のそれぞれに対して準同型である写像を意味する。この例では、写像 $\theta(g, h)$ は、群 G の元 g に対して準同型であ

り、かつ、群Hの元hに対して準同型である。

[0085] 依頼装置1'と計算装置2'の間には通信路が確立されており、依頼装置1'及び計算装置2'は双方向に通信可能である。この通信路は秘密に保たれている必要はなく、第三者がこの通信路を流れる情報を傍受することができてもよい。

[0086] 依頼装置1'は信頼できない計算装置2'に乱数によって攪乱した情報を送信し、計算装置2'はその攪乱された情報を用いて一定のアルゴリズムに従って計算を行い、その計算結果を依頼装置1'に返信する。この計算装置2'への情報の送受信を繰り返すことにより、依頼装置1'は最終的に $\theta(g, h)$ を計算する。

[0087] 依頼装置1'は、まずステップS11'からステップS125'（図15）の処理により $\theta(g, \mu_h)$ と同等の情報 (σ, ν') を計算し、その $\theta(g, \mu_h)$ と同等の情報 (σ, ν') を用いてステップS21'からステップS225'の処理により $\theta(g, \mu)$ を計算する。

[0088] 依頼装置1'は、図12及び図13に例示する、第一乱数生成部11'、第二乱数生成部12'、第一入力情報計算部13'、第二入力情報計算部14'、第一リスト情報計算部15'、第一リスト記憶部16'、受信部17'、送信部18'、第四乱数生成部21'、第五乱数生成部22'、第三入力情報計算部23'、第四入力情報計算部24'、第二リスト情報計算部25'、第二リスト記憶部26'、第三乱数生成部27'、第一判定部28'、第六乱数生成部31'、第七乱数生成部32'、第五入力情報計算部33'、第六入力情報計算部34'、第三リスト情報計算部35'、第三リスト記憶部36'、第九乱数生成部41'、第十乱数生成部42'、第七入力情報計算部43'、第八入力情報計算部44'、第四リスト情報計算部45'、第四リスト計算部46'、第八乱数生成部47'及び第二判定部48'を例えば含む。

[0089] 計算装置2'は、図14に例示するように、受信部51'、送信部52'、第一出力情報計算部53'、第二出力情報計算部54'、第三出力情報計

算部 5 5' 及び第四出力情報計算部 5 6' を例えば含む。

[0090] <ステップ S 1 1' (図 1 5) >

第一乱数生成部 1 1' は、0 以上 K_G 未満の整数の一樣乱数である r_1 を生成する (ステップ S 1 1')。生成された乱数 r_1 は、第一入力情報計算部 1 3' 及び第一リスト情報計算部 1 5' に送られる。

[0091] <ステップ S 1 2' >

第二乱数生成部 1 2' は、0 以上 K_H 未満の整数の一樣乱数である r_2 を生成する (ステップ S 1 2')。生成された乱数 r_2 は、第二入力情報計算部 1 4'、第一リスト情報計算部 1 5' 及び第一リスト記憶部 1 6' に送られる。

[0092] <ステップ S 1 3' >

第一入力情報計算部 1 3' は、第一入力情報 $g_1 = \mu_g^{r_1} g$ を計算する (ステップ S 1 3')。計算された g_1 は送信部 1 8' に送られる。

ここで、 μ_g の右肩の r_1 は、 r_1 のことである。このように、この出願において、 α を第一の文字、 β を第二の文字、 γ を数字として、 $\alpha^{\beta\gamma}$ と表記した場合には、その $\beta\gamma$ は β_γ 、すなわち β の下付き γ を意味する。

[0093] また、 $g_1 = \mu_g^{r_1} g$ を計算するとは、 $\mu_g^{r_1} g$ という式で定義される g_1 の値を計算することである。式 $\mu_g^{r_1} g$ の値を最終的に計算することができれば、途中の計算方法は問わない。これは、この出願で登場する他の式の計算についても同様である。

[0094] <ステップ S 1 4' >

第二入力情報計算部 1 4' は、第二入力情報 $h_1 = \mu_h^{r_2}$ を計算する (ステップ S 1 4')。計算された h_1 は送信部 1 8' に送られる。

[0095] <ステップ S 1 5' >

送信部 1 8' は、第一入力情報 g_1 及び第二入力情報 h_1 を計算装置 2' に送信する (ステップ S 1 5')。

[0096] <ステップ S 1 6' >

計算装置 2' の受信部 5 1' (図 1 4) は、第一入力情報 g_1 及び第二入力

情報 h_1 を受信する（ステップS 1 6'）。

[0097] <ステップS 1 7'>

第一出力情報計算部5 3'は、第一入力情報 g_1 及び第二入力情報 h_1 を用いて計算を行い、その計算結果を第一出力情報 z_1 とする（ステップS 1 7'）。 z_1 は、送信部5 2'に送られる。

[0098] 第一出力情報計算部5 3'は、 $\theta(g_1, h_1)$ を計算可能である。第一出力情報計算部5 3'による計算の結果が $\theta(g_1, h_1)$ であることもあれば、 $\theta(g_1, h_1)$ でないこともある。

[0099] この出願において、計算可能とは、無視することができない確率で計算することができることを意味する。無視することができない確率とは、セキュリティパラメータ k についての広義単調増加関数である多項式を多項式 $f(k)$ として、 $1/f(k)$ 以上の確率である。

[0100] <ステップS 1 8'>

送信部5 2'は、第一出力情報 z_1 を依頼装置1'に送信する（ステップS 1 8'）。

[0101] <ステップS 1 9'>

依頼装置1'の受信部1 7'（図1 2）は、第一出力情報 z_1 を受信する（ステップS 1 9'）。受信した第一出力情報 z_1 は、第一リスト情報計算部1 5'に送られる。ここでは、第一出力情報 z_1 は群 F の元であるとする。

[0102] <ステップS 1 1 0'>

第一リスト情報計算部1 5'は、乱数 r_1 、乱数 r_2 及び第一出力情報 z_1 を用いて、 $z_1 \nu^{-r_1 r_2}$ を計算する（ステップS 1 1 0'）。計算された $z_1 \nu^{-r_1 r_2}$ は、第一リスト記憶部1 6'に送られる。

[0103] <ステップS 1 1 1'>

乱数 r_2 と、 $z_1 \nu^{-r_1 r_2}$ とから構成される情報の組 $(r_2, z_1 \nu^{-r_1 r_2})$ がリスト L_1 に追加される。この例では、第一リスト記憶部1 6'に、情報の組 $(r_2, z_1 \nu^{-r_1 r_2})$ が記憶される（ステップS 1 1 1'）。

[0104] <ステップS 1 1 2'>

第三乱数生成部 27' は、0 以上 K 未満の整数の一樣乱数である d_1 を生成する（ステップ S 112'）。生成された乱数 d_1 は、第三入力情報計算部 23' 及び第二リスト記憶部 26' に送られる。

[0105] <ステップ S 113'>

第四乱数生成部 21' は、0 以上 K_G 未満の整数の一樣乱数である r_4 を生成する（ステップ S 113'）。生成された乱数 r_4 は、第三入力情報計算部 23' 及び第二リスト情報計算部 25' に送られる。

[0106] <ステップ S 114'>

第五乱数生成部 22' は、0 以上 K_H 未満の整数の一樣乱数である r_5 を生成する（ステップ S 114'）。生成された乱数 r_5 は、第四入力情報計算部 24'、第二リスト情報計算部 25' 及び第二リスト記憶部 26' に送られる。

[0107] <ステップ S 115'>

第三入力情報計算部 23' は、第三入力情報 $g_2 = \mu_g r_4 g^{d1}$ を計算する（ステップ S 115'）。計算された第三入力情報 g_2 は、送信部 18' に送られる。

[0108] <ステップ S 116'>

第四入力情報計算部 24' は、第四入力情報 $h_2 = \mu_h r_5$ を計算する（ステップ S 116'）。計算された第四入力情報 h_2 は、送信部 18' に送られる。

[0109] <ステップ S 117'>

送信部 18' は、第三入力情報 g_2 及び第四入力情報 h_2 を計算装置 2' に送信する（ステップ S 117'）。

[0110] <ステップ S 118'>

計算装置 2' の受信部 51'（図 14）は、第三入力情報 g_2 及び第四入力情報 h_2 を受信する（ステップ S 118'）。

[0111] <ステップ S 119'>

第二出力情報計算部 54' は、第三入力情報 g_2 及び第三入力情報 h_2 を用

いて計算を行い、その計算結果を第二出力情報 z_2 とする（ステップ S 1 1 9'）。 z_2 は、送信部 5 2' に送られる。

第二出力情報計算部 5 4' は、 $\theta(g_2, h_2)$ を計算可能である。第二出力情報計算部 5 4' による計算の結果が $\theta(g_2, h_2)$ であることもあれば、 $\theta(g_2, h_2)$ でないこともある。

[0112] <ステップ S 1 2 0'>

送信部 5 2' は、第二出力情報 z_2 を依頼装置 1' に送信する（ステップ S 1 2 0'）。

[0113] <ステップ S 1 2 1'>

依頼装置 1' の受信部 1 7'（図 1 2）は、第二出力情報 z_2 を受信する（ステップ S 1 2 1'）。受信した第二出力情報 z_2 は、第二リスト情報計算部 2 5' に送られる。ここでは、第二出力情報 z_2 は群 F の元であるとする。

[0114] <ステップ S 1 2 2'>

第二リスト情報計算部 2 5' は、乱数 r_4 、乱数 r_5 及び第二出力情報 z_2 を用いて、 $z_2 \nu^{-r_4 r_5}$ を計算する（ステップ S 1 2 2'）。計算された $z_2 \nu^{-r_4 r_5}$ は、第二リスト記憶部 2 6' に送られる。

[0115] <ステップ S 1 2 3'>

乱数 d_1 と、乱数 r_5 と、 $z_2 \nu^{-r_4 r_5}$ とから構成される情報の組（ $d_1, r_5, z_2 \nu^{-r_4 r_5}$ ）が、リスト L_2 に追加される。この例では、第二リスト記憶部 2 6' には、情報の組（ $d_1, r_5, z_2 \nu^{-r_4 r_5}$ ）が記憶される（ステップ S 1 2 3'）。

[0116] <ステップ S 1 2 4'>

第一判定部 2 8' は、第一リスト記憶部 1 6' から読み込んだ情報の組の第一成分を s_1 とし、第二成分を w_1 とし、第二リスト記憶部 2 6' から読み込んだ情報の組の第一成分を t_2 とし、第二成分を s_2 とし、第三成分を w_2 とし、これらの情報の組が $(w_1)^\wedge (t_2 s_2 s_1^{-1}) = w_2$ の関係を満たすかを判定する（ステップ S 1 2 4'）。

[0117] 第一判定部 2 8' は、第一リスト記憶部 1 6' 及び第二リスト記憶部 2 6

’に複数の情報の組が記憶されている場合には、第一リスト記憶部16’に記憶された情報の組 $(r_2, z_1 \nu^{-r_1 r_2})$ と、第二リスト記憶部26’に記憶された情報の組 $(d_1, r_5, z_2 \nu^{-r_4 r_5})$ とから構成されるすべての情報のペアについて、上記関係を満たすかどうかを判定する。もちろん、既に上記関係を満たすかどうかを判定した情報のペアについては、その判定処理を省いてもよい。

[0118] <ステップS125’>

第一判定部28’は、上記の関係を満たす場合には、 s_1 を σ に代入し、 w_1 を ν' に代入する(ステップS125’)。ここで、 $\nu'^{1/\sigma} = w_1^{1/\sigma} = \theta(g, \mu_h)$ となる。 $\nu'^{1/\sigma} = \theta(g, \mu_h)$ となる理由については後述する。

上記の関係を満たさない場合には、ステップS11’に戻る。

[0119] <ステップS21’ (図16)>

第六乱数生成部31’は、0以上 K_g 未満の整数の一樣乱数である r_6 を生成する(ステップS21’)。生成された乱数 r_6 は、第五入力情報計算部33’、第三リスト情報計算部35’及び第三リスト記憶部36’に送られる。

[0120] <ステップS22’>

第七乱数生成部32’は、0以上 K_h 未満の整数の一樣乱数である r_7 を生成する(ステップS22’)。生成された乱数 r_7 は、第六入力情報計算部34’及び第三リスト情報計算部35’に送られる。

[0121] <ステップS23’>

第五入力情報計算部33’は、第五入力情報 $g_3 = \mu_g r_6$ を計算する(ステップS23’)。計算された g_3 は送信部18’に送られる。

[0122] <ステップS24’>

第六入力情報計算部34’は、第六入力情報 $h_3 = \mu_h r_7^\sigma h$ を計算する(ステップS24’)。計算された h_3 は送信部18’に送られる。

[0123] <ステップS25’>

送信部 18' は、第五入力情報 g_3 及び第六入力情報 h_3 を計算装置 2' に送信する（ステップ S25'）。

[0124] <ステップ S26'>

計算装置 2' の受信部 51'（図 14）は、第五入力情報 g_3 及び第六入力情報 h_3 を受信する（ステップ S26'）。

[0125] <ステップ S27'>

第三出力情報計算部 55' は、第五入力情報 g_3 及び第六入力情報 h_3 を用いて計算を行い、その計算結果を第三出力情報 z_3 とする（ステップ S27'）。 z_3 は、送信部 52' に送られる。

第三出力情報計算部 55' は、 $\theta(g_3, h_3)$ を計算可能である。第三出力情報計算部 55' による計算の結果が $\theta(g_3, h_3)$ であることもあれば、 $\theta(g_3, h_3)$ でないこともある。

[0126] <ステップ S28'>

送信部 52' は、第三出力情報 z_3 を依頼装置 1' に送信する（ステップ S28'）。

[0127] <ステップ S29'>

依頼装置 1' の受信部 17'（図 13）は、第三出力情報 z_3 を受信する（ステップ S29'）。受信した第三出力情報 z_3 は、第三リスト情報計算部 35' に送られる。ここでは、第三出力情報 z_3 は群 F の元であるとする。

[0128] <ステップ S210'>

第三リスト情報計算部 35' は、乱数 r_6 、乱数 r_7 及び第三出力情報 z_3 を用いて、 $z_3 \nu'^{-r_6 r_7}$ を計算する（ステップ S210'）。計算された $z_3 \nu'^{-r_6 r_7}$ は、第三リスト記憶部 36' に送られる。

[0129] <ステップ S211'>

乱数 r_6 と、 $z_3 \nu'^{-r_6 r_7}$ とから構成される情報の組 $(r_6, z_3 \nu'^{-r_6 r_7})$ がリスト L_3 に追加される。この例では、第三リスト記憶部 36' に、情報の組 $(r_6, z_3 \nu'^{-r_6 r_7})$ が記憶される（ステップ S211'）。

[0130] <ステップ S212'>

第八乱数生成部 47' は、0 以上 K 未満の整数の一樣乱数である d_2 を生成する（ステップ S 212'）。生成された乱数 d_2 は、第八入力情報計算部 44 及び第四リスト記憶部 46' に送られる。

[0131] <ステップ S 213'>

第九乱数生成部 41' は、0 以上 K_G 未満の整数の一樣乱数である r_9 を生成する（ステップ S 213'）。生成された乱数 r_9 は、第七入力情報計算部 43'、第四リスト情報計算部 45' 及び第四リスト記憶部 46' に送られる。

[0132] <ステップ S 214'>

第十乱数生成部 42' は、0 以上 K_H 未満の整数の一樣乱数である r_{10} を生成する（ステップ S 214'）。生成された乱数 r_{10} は、第八入力情報計算部 44'、第四リスト情報計算部 45' 及び第四リスト記憶部 46' に送られる。

[0133] <ステップ S 215'>

第七入力情報計算部 43' は、第七入力情報 $g_4 = g^{r_9}$ を計算する（ステップ S 215'）。計算された第七入力情報 g_4 は、送信部 18' に送られる。

[0134] <ステップ S 216'>

第八入力情報計算部 44' は、第八入力情報 $h_4 = \mu_h^{r_{10}\sigma} h^{d_2}$ を計算する（ステップ S 216'）。計算された第八入力情報 h_4 は、送信部 18' に送られる。

[0135] <ステップ S 217'>

送信部 18' は、第七入力情報 g_4 及び第八入力情報 h_4 を計算装置 2' に送信する（ステップ S 217'）。

[0136] <ステップ S 218'>

計算装置 2' の受信部 51'（図 14）は、第七入力情報 g_4 及び第八入力情報 h_4 を受信する（ステップ S 218'）。

[0137] <ステップ S 219'>

第四出力情報計算部 56' は、第七入力情報 g_4 及び第八入力情報 h_4 を用

いて計算を行い、その計算結果を第四出力情報 z_4 とする（ステップ S 2 1 9'）。 z_4 は、送信部 5 2' に送られる。

第四出力情報計算部 5 6' は、 $\theta(g_4, h_4)$ を計算可能である。第四出力情報計算部 5 6' による計算の結果が $\theta(g_4, h_4)$ であることもあれば、 $\theta(g_4, h_4)$ でないこともある。

[0138] <ステップ S 2 2 0'>

送信部 5 2' は、第四出力情報 z_4 を依頼装置 1' に送信する（ステップ S 2 2 0'）。

[0139] <ステップ S 2 2 1'>

依頼装置 1' の受信部 1 7'（図 1 2）は、第四出力情報 z_4 を受信する（ステップ S 2 2 1）。受信した第四出力情報 z_4 は、第四リスト情報計算部 4 5' に送られる。ここでは、第四出力情報 z_4 は群 F の元であるとする。

[0140] <ステップ S 2 2 2'>

第四リスト情報計算部 4 5' は、乱数 r_9 、乱数 r_{10} 及び第四出力情報 z_4 を用いて、 $z_4 \nu^{-r_9 r_{10}}$ を計算する（ステップ S 2 2 2'）。計算された $z_4 \nu^{-r_9 r_{10}}$ は、第四リスト記憶部 4 6' に送られる。

[0141] <ステップ S 2 2 3'>

乱数 d_2 と、乱数 r_9 と、 $z_4 \nu^{-r_9 r_{10}}$ とから構成される情報の組 $(d_2, r_9, z_4 \nu^{-r_9 r_{10}})$ が、リスト L_4 に追加される。この例では、第四リスト記憶部 4 6' に、情報の組 $(d_2, r_9, z_4 \nu^{-r_9 r_{10}})$ が記憶される（ステップ S 2 2 3'）。

[0142] <ステップ S 2 2 4'>

第二判定部 4 8' は、第三リスト記憶部 3 6' から読み込んだ情報の組の第一成分を s_3 とし、第二成分を w_3 とし、第四リスト記憶部 4 6' から読み込んだ情報の組の第一成分を t_4 とし、第二成分を s_4 とし、第三成分を w_4 とし、これらの情報の組が $(w_3)^{\wedge} (t_4 s_4 s_3^{-1}) = w_4$ の関係を満たすかを判定する（ステップ S 2 2 4'）。

[0143] 第二判定部 4 8' は、第三リスト記憶部 3 6' 及び第四リスト記憶部 4 6

’に複数の情報の組が記憶されている場合には、第三リスト記憶部36’に記憶された情報の組 $(r_6, z_3 \nu' - r_6 r_7)$ と、第四リスト記憶部46’に記憶された情報の組 $(d_2, r_9, z_4 \nu' - r_9 r_{10})$ とから構成されるすべての情報のペアについて、上記関係を満たすかどうかを判定する。もちろん、既に上記関係を満たすかどうかを判定した情報のペアについては、その判定処理を省いてもよい。

[0144] <ステップS225’>

第二判定部48’は、上記の関係を満たす場合には、 $(w_3)^{\wedge (s_3^{-1})}$ を出力する(ステップS225’)。ここで、 $(w_3)^{\wedge (s_3^{-1})} = \theta(g, h)$ となる。 $(w_3)^{\wedge (s_3^{-1})} = \theta(g, h)$ となる理由については後述する。

上記の関係を満たさない場合には、ステップS21’に戻る。

[0145] $(w_3)^{\wedge (s_3^{-1})}$ の計算、すなわち w_3 のべき乗根の計算が困難な場合には、次のようにして $\theta(g, h)$ を容易に計算することができる。第二判定部48’は、ステップS21’からステップS224’の処理を繰り返して $(w_3)^{\wedge (t_4 s_4 s_3^{-1})} = w_4$ の関係を満たす w_3 と s_3 との組 (w_3, s_3) を順次 $(\alpha_1, S_1), (\alpha_2, S_2), \dots, (\alpha_m, S_m), \dots$ として記憶部410’に記憶する。 m は自然数である。第二判定部48’は、 S_1 と互いに素となる S_m が見つければ、 L_1 と L_2 とを整数として $L_1 S_1 + L_2 S_m = 1$ となる L_1 及び L_2 を計算して、その L_1 及び L_2 を用いて $\alpha_1^{L_1} \alpha_m^{L_2}$ を計算する。 $\alpha_1^{L_1} \alpha_m^{L_2} = \theta(g, h)^{(L_1 S_1 + L_2 S_2)} = \theta(g, h)$ となる。また、第二判定部48’は、 $S_1, S_2, \dots, S_m$ の最小公倍数が1になれば、 $L_1, L_2, \dots, L_m$ を整数として $L_1 S_1 + L_2 S_2 + \dots + L_m S_m = 1$ となる $L_1, L_2, \dots, L_m$ を計算して、その $L_1, L_2, \dots, L_m$ を用いて $\alpha_1^{L_1} \alpha_2^{L_2} \dots \alpha_m^{L_m}$ を計算してもよい。 $\alpha_1^{L_1} \alpha_2^{L_2} \dots \alpha_m^{L_m} = \theta(g, h)^{(L_1 S_1 + L_2 S_2 + \dots + L_m S_m)} = \theta(g, h)$ となる。

[0146] 依頼装置1’と計算装置2’との間の通信を傍受することができる攻撃者Mがいるとしても、依頼装置1’及び計算装置2’との間で通信される情報

を、依頼装置 1' のみを知る乱数（例えば、 r_1, r_2 ）で攪乱することにより、攻撃者 M から秘匿することができる。

[0147] また、依頼装置 1' 及び計算装置 2' との間で通信される情報は依頼装置 1' のみを知る r_1, r_2 等の乱数で攪乱されているため、計算装置 2' は、依頼装置 1' が最終的に計算しようとする $\theta(g, h)$ はもちろんのこと、その入力である g 及び h をも知ることはできない。

[0148] したがって、計算装置 2' は信頼することができる計算機である必要はなく、双準同型写像を計算するためのシステムの構成要件を緩和することができる。また、信頼することができる計算機は一般に高価であり運用に費用を要するが、計算装置 2' が信頼することができる計算機である必要ないため、双準同型写像を計算するためのシステムの構築及び運用のコストを削減することができる。

[0149] ≪ $\nu'^{1/\sigma} = \theta(g, \mu_h)$ となる理由について≫

まず、`randomizable sampler` と呼ばれる確率変数 S_X (d) について説明する。 $w \in F$ に関する誤差 X の `randomizable sampler` である確率変数 $S_X(d)$ は、 $S_X(d) = w^d X$ である。 d は自然数である。

[0150] ここで、 R_1, R_2, R_1' 及び R_2' を乱数として、計算装置が $g^d \mu_g^{R_1}$ 及び $\mu_h^{R_2}$ を用いて行う計算の計算結果を $B(g^d \mu_g^{R_1}, \mu_h^{R_2})$ （計算装置が依頼装置に返す計算結果を z とすると、 $z = B(g^d \mu_g^{R_1}, \mu_h^{R_2})$ である。）とし、群 F に値を持つ確率変数 X を $X = B(\mu_g^{R_1'}, \mu_h^{R_2'})^{1/R_2'} \theta(\mu_g^{R_1'}, \mu_h)^{-1}$ と定義すると、 $S_X(d) = z^{(1/R_2')} \nu^{-R_1}$ は、 $\theta(g, \mu_h)$ に関する誤差 X の `randomizable sampler` となる。

[0151] $S_X(d) = z^{(1/R_2')} \nu^{-R_1} = B(g^d \mu_g^{R_1}, \mu_h^{R_2})^{1/R_2'} \theta(\mu_g, \mu_h)^{-R_1} = X \theta(g^d \mu_g^{R_1}, \mu_h) \theta(\mu_g^{R_1}, \mu_h)^{-1} = X \theta(g^d, \mu_h) \theta(\mu_g^{R_1}, \mu_h) \theta(\mu_g^{R_1}, \mu_h)^{-1} = \theta(g, \mu_h)^d X$ であるためである。

[0152] 上記式展開において、 $X = B(\mu_g^{R_1'}, \mu_h^{R_2'})^{1/R_2'} \theta(\mu_g^{R_1'}, \mu_h$

$)^{-1} = B(g^d \mu_g^{R1}, \mu_h^{R2})^{1/R2} \theta(g^d \mu_g^{R1}, \mu_h)^{-1}$ であり、 $B(g^d \mu_g^{R1}, \mu_h^{R2})^{1/R2} = X \theta(g^d \mu_g^{R1}, \mu_h)$ であるという性質を用いている。この性質は、 R_1 、 R_2 、 R_1' 及び R_2' が乱数であることに基づく。

[0153] ここで、 $S_X(1)$ の実現値を $\theta(g, \mu_h)^{1x_1}$ と表記し、 $S_X(d)$ の実現値を $\theta(g, \mu_h)^{dx_2}$ と表記するとして、 $S_X(1)$ の実現値の d 乗 $= S_X(d)$ の実現値、すなわち $(\theta(g, \mu_h)^{1x_1})^d = \theta(g, \mu_h)^{dx_2}$ となるのは、 x_1 及び x_2 が群 F の単位元 e_f のときである可能性が非常に高いことを発明者は見出した。ここでは、その証明は省略する。 x_1 が群 F の単位元 e_f のとき、 $S_X(1)$ の実現値 $= \theta(g, \mu_h)^{1x_1} = \theta(g, \mu_h)$ となる。

[0154] 上記実施形態の代理計算システムは、この *randomizable sampler* の性質を用いている。

[0155] ステップ $S11'$ からステップ $S111'$ の処理が $S_X(1)$ の実現値 $\theta(g, \mu_h)^{1x_1}$ の計算に対応している。実際には、 $S_X(1)$ の実現値自体は計算していないが、同処理により得られる $(r_2, z_1 \nu^{-r1r2})$ を用いて、 $z_1 \nu^{-r1r2}$ を $1/r_2$ 乗すると、 $(z_1 \nu^{-r1r2})^{1/r2} = z_1^{1/r2} \nu^{-r1}$ となり、 $S_X(1)$ の実現値 $\theta(g, \mu_h)^{1x_1}$ となる。同様に、ステップ $S112'$ からステップ $S123'$ の処理が $S_X(d_1)$ の実現値 $\theta(g, \mu_h)^{d1x_2}$ の計算に対応している。

[0156] また、ステップ $S124'$ の処理が、 $S_X(1)$ の実現値の d_1 乗 $= S_X(d_1)$ 、すなわち $(\theta(g, \mu_h)^{1x_1})^{d1} = \theta(g, \mu_h)^{d1x_2}$ であるかどうかの判定に対応している。ステップ $S124$ で用いる判定条件 $(w_1)^{\wedge}(t_2 s_2 s_1^{-1})$ は、 $(w_1)^{\wedge}(t_2 s_2 s_1^{-1}) = w_2 \Leftrightarrow (w_1^{1/s1})^{t2} = w_2^{1/s2} \Leftrightarrow (z_1^{1/r2} \nu^{-r1})^{d1} = z_2^{1/r5} \nu^{-r4} \Leftrightarrow (\theta(g, \mu_h)^{1x_1})^{d1} = \theta(g, \mu_h)^{d1x_2} \Leftrightarrow S_X(1)$ の実現値の d_1 乗 $= S_X(d_1)$ の実現値であるためである。ここで、定義より $s_1 = r_2$ 、 $w_1 = z_1 \nu^{-r1r2}$ 、 $t_2 = d_1$ 、 $s_2 = r_5$ 、 $w_2 = z_2 \nu^{-r4r5}$ である。

[0157] さらに、ステップ $S125'$ における σ 及び ν' が、 $\theta(g, \mu_h)$ に対応

している。上記したように $S_x(1)$ の実現値の d_1 乗 $=S_x(d_1)$ の実現値のとき、 $\nu'^{1/\sigma} = w_1^{1/s_1} = z_1^{1/r_2} \nu^{-r_1} = \theta(g, \mu_h)^{1/x_1} = \theta(g, \mu_h)$ であるためである。

[0158] $\ll (w_3)^{\wedge} (s_3^{-1}) = \theta(g, h)$ となる理由について

R_1, R_2, R_1' 及び R_2' を乱数として、計算装置が g^{R_1} 及び $h^d \mu_h^{R_2}$ を用いて行う計算の計算結果を $B(g^{R_1}, h^d \mu_h^{R_2})$ (計算装置が依頼装置に返す計算結果を z とすると、 $z = B(g^{R_1}, h^d \mu_h^{R_2})$ である。) とし、群 F に値を持つ確率変数 X を $X = B(g^{R_1'}, \mu_h^{R_2'})^{1/R_1'} \theta(g, \mu_h^{R_2'})^{-1}$ と定義すると、 $S_x(d) = z^{(1/R_1)} \nu'^{-R_2}$ は、 $\theta(g, h)$ に関する誤差 X の *randomizable sampler* となる。

[0159] $S_x(d) = z^{(1/R_1)} \nu'^{-R_2} = B(g^{R_1}, h^d \mu_h^{R_2})^{1/R_1} \theta(g, \mu_h)^{-R_2} = X \theta(g, h^d \mu_h^{R_2}) \theta(g, \mu_h^{R_2})^{-1} = X \theta(g, h^d) \theta(g, \mu_h^{R_2}) \theta(g, \mu_h^{R_2})^{-1} = \theta(g, h)^d X$ であるためである。

[0160] 上記式展開において、 $X = B(g^{R_1'}, \mu_h^{R_2'})^{1/R_1'} \theta(g, \mu_h^{R_2'})^{-1} = B(g^{R_1}, \mu_h^{R_2})^{1/R_1} \theta(g, h^d \mu_h^{R_2})^{-1}$ であり、 $B(g^{R_1}, h^d \mu_h^{R_2})^{1/R_1} = X \theta(g, h^d \mu_h^{R_2})$ であるという性質を用いている。この性質は、 R_1, R_2, R_1' 及び R_2' が乱数であることに基づく。

[0161] ここで、 $S_x(1)$ の実現値を $S_x(1) = \theta(g, h)^{1/x_1}$ と表記し、 $S_x(d)$ の実現値を $S_x(d) = \theta(g, h)^d x_2$ と表記するとして、 $S_x(1)$ の実現値の d 乗 $= S_x(d)$ 、すなわち $(\theta(g, h)^{1/x_1})^d = \theta(g, h)^d x_2$ となるのは、 x_1 及び x_2 が群 F の単位元 e_f のときである可能性が非常に高いことを発明者は見出した。ここでは、その証明は省略する。 x_1 が群 F の単位元 e_f のとき、 $S_x(1)$ の実現値 $= \theta(g, h)^{1/x_1} = \theta(g, h)$ となる。

[0162] 上記実施形態の代理計算システムは、この *randomizable sampler* の性質を用いている。

[0163] ステップ $S21'$ からステップ $S211'$ の処理が $S_x(1)$ の実現値 $\theta(g, h)^{1/x_1}$ の計算に対応している。実際には、 $S_x(1)$ の実現値自体は計

算していないが、同処理により得られる $(r_6, z_3 \nu' - r_6 r_7)$ を用いて、
 $z_3 \nu' - r_6 r_7$ を $1/r_6$ 乗すると、 $(z_3 \nu' - r_6 r_7)^{1/r_6} = z_3^{1/r_6} \nu' - r_7$ となり、 $S_X(1)$ の実現値 $\theta(g, h)^{1 \times 1}$ となる。同様に、ステップ S 2 1 2' からステップ S 2 2 3' の処理が $S_X(d_2)$ の実現値 $\theta(g, h)^{d_2 \times 2}$ の計算に対応している。

[0164] また、ステップ S 2 2 4' の処理が、 $S_X(1)$ の実現値の d_2 乗 $= S_X(d_2)$ の実現値、すなわち $(\theta(g, h)^{1 \times 1})^{d_2} = \theta(g, h)^{d_2 \times 2}$ であるかどうかの判定に対応している。ステップ S 2 2 4' で用いる判定条件 $(w_3)^{\wedge}(t_4 s_4 s_3^{-1}) = w_4$ は、 $(w_3)^{\wedge}(t_4 s_4 s_3^{-1}) = w_4 \Leftrightarrow (w_3^{1/s_3})^{t_4} = w_4^{1/s_4} \Leftrightarrow (z_3^{1/r_6} \nu' - r_7)^{d_2} = z_4^{1/r_9} \nu' - r_{10} \Leftrightarrow (\theta(g, h)^{1 \times 1})^{d_2} = \theta(g, h)^{d_2 \times 2} \Leftrightarrow S_X(1)$ の実現値の d_2 乗 $= S_X(d_2)$ の実現値であるためである。ここで、定義より $s_3 = r_6$ 、 $w_3 = z_3 \nu' - r_6 r_7$ 、 $t_4 = d_2$ 、 $s_4 = r_9$ 、 $w_4 = z_4 \nu' - r_9 r_{10}$ である。

[0165] さらに、ステップ S 2 2 5' における $(w_3)^{\wedge}(s_3^{-1})$ が、 $\theta(g, h)$ に対応している。上記したように $S_X(1)$ の実現値の d_2 乗 $= S_X(d_2)$ の実現値のとき、 $(w_3)^{\wedge}(s_3^{-1}) = (z_3 \nu' - r_6 r_7)^{\wedge}(r_6^{-1}) = z_3^{1/r_6} \nu' - r_7 = \theta(g, h)^{1 \times 1} = \theta(g, h)$ であるためである。

[0166] [第五実施形態]

第五実施形態の代理計算システムは、ステップ S 1 3'、ステップ S 1 1 0' 及びステップ S 1 1 1' が第四実施形態の代理計算システムとは異なり、他の部分については第四実施形態の代理計算システムと同様である。以下、第四実施形態と異なる部分を中心に説明する。

[0167] 第一入力情報計算部 1 3' は、 $g_1 = \mu_g r_1 g$ ではなく、 $g_1 = g r_1$ で定義される第一入力情報を計算する（ステップ S 1 3'）。

第一リスト情報計算部 1 5' は、 $z_1 \nu - r_1 r_2$ ではなく、乱数 r_1 及び乱数 r_2 を用いて $r_1 r_2$ を計算して、その計算結果を第一リスト記憶部 1 6' に送る（ステップ S 1 1 0'）。

第一リスト記憶部 1 6' には、情報の組 $(r_2, z_1 \nu - r_1 r_2)$ ではなく、

計算された $r_1 r_2$ と計算装置 2' から受信した $z_1 \in F$ とから構成される情報の組 $(r_1 r_2, z_1)$ が記憶される (ステップ S 1 1 1')。

- [0168] 第四実施形態のステップ S 1 1 0' では、 $z_1 \nu^{-r_1 r_2}$ という群 F のべき演算を行う必要があったが、第五実施形態のステップ S 1 1 0' では $r_1 r_2$ の計算を行っておりべき演算の回数が 1 回減っている。このように、べき演算の回数を減らすことにより演算の効率性を増すことができる。また、群 G 、群 H において非自明べき根の計算が困難であるならば、第四実施形態と比較して安全性は低下しない。

[0169] [第六実施形態]

第六実施形態の代理計算システムは、ステップ S 2 4'、ステップ S 2 1 0' 及びステップ S 2 1 1' が第四実施形態の代理計算システムとは異なり、他の部分については第四実施形態の代理計算システムと同様である。以下、第四実施形態と異なる部分を中心に説明する。

- [0170] 第六入力情報計算部 3 4' は、 $h_3 = \mu_h r^7 \sigma h$ ではなく、 $h_3 = h r^7$ で定義される第六入力情報 h_3 を計算する (ステップ S 2 4')。

第三リスト情報計算部 3 5' は、 $z_3 \nu'^{-r_6 r_7}$ ではなく、乱数 r_6 及び乱数 r_7 を用いて $r_6 r_7$ を計算する (ステップ S 2 1 0')。

第三リスト記憶部 3 6' には、情報の組 $(r_6, z_3 \nu'^{-r_6 r_7})$ ではなく、計算された $r_6 r_7$ と計算装置 2' から受信した $z_3 \in F$ とから構成される情報の組 $(r_6 r_7, z_3)$ が記憶される (ステップ S 2 1 1')。

- [0171] 第四実施形態のステップ S 2 1 0' では、 $z_3 \nu'^{-r_6 r_7}$ という群 F のべき演算を行う必要があったが、第六実施形態のステップ S 2 1 0' では $r_6 r_7$ の計算を行っておりべき演算の回数が 1 回減っている。このように、べき演算の回数を減らすことにより演算の効率性を増すことができる。

- [0172] 群 G 、群 H において非自明べき根の計算が困難であるならば、第四実施形態と比較して安全性は低下しない。

[0173] [第七実施形態]

第七実施形態の代理計算システムは、ステップ S 1 2 5' 及びステップ S

2 1 4' が第四実施形態の代理計算システムとは異なり、他の部分については第四実施形態の代理計算システムと同様である。以下、第四実施形態と異なる部分を中心に説明する。

第一判定部 2 8' は、上記の関係を満たす場合には、 $t_1 s_2$ を σ に代入し、 w_2 を ν' に代入する（ステップ S 1 2 5'）。

第十乱数生成部 4 2' は、乱数 r_9 を用いて $-r_9^{-1}$ を計算して r_{10} とする（ステップ S 2 1 4'）。

[0174] このように、 ν' の定義を変更して、 σ を計算装置 2' にとって推測が困難な乱数とすることにより安全性が増す。また、乱数 r_9 を用いて乱数 r_{10} を計算することにより、乱数を生成する回数を減らすことができる。乱数 r_{10} が乱数 r_9 により定まるため第八入力情報 $h_4 = \mu_h r^{10\sigma} h^{d2}$ の乱雑性が低下し安全性が損なわれるとも思われるが、第八入力情報 $h_4 = \mu_h r^{10\sigma} h^{d2}$ は乱数 r_{10} だけでなく更に σ により攪乱されているため安全性は損なわれない。

[0175] なお、第七実施形態においては更にステップ S 2 2' 及びステップ S 2 1 1' を以下のように変更してもよい。

[0176] 第七乱数生成部 3 2' は、乱数 r_6 を用いて $-r_6^{-1}$ を計算して r_7 とする（ステップ S 2 2'）。

第三リスト記憶部 3 6' には、1 と上記計算された $z_3 \nu' - r_6 r_7$ とから構成される情報の組（1, $z_3 \nu' - r_6 r_7$ ）が記憶される（ステップ S 2 1 1'）。

[0177] このように、乱数 r_6 を用いて乱数 r_7 を計算することにより乱数を生成する回数を減らすことができる。

群 G、群 H において非自明べき根の計算が困難であるならば、第四実施形態と比較して安全性は低下しない。

[0178] [第八実施形態]

第八実施形態の代理計算システムは、ステップ S 1 1 3' が第四実施形態の代理計算システムとは異なり、他の部分については第四実施形態の代理計算システムと同様である。以下、第四実施形態と異なる部分を中心に説明す

る。

[0179] まず、ステップS 1 1 3' に先立ち、第五乱数生成部 2 2' は乱数 r_5 を生成する（ステップS 1 1 4' ）。

第四乱数生成部 2 1' は、乱数 r_5 を用いて $-r_5^{-1}$ を計算して r_4 とする（ステップS 1 1 3' ）。

このように、乱数 r_5 を用いて乱数 r_4 を計算することにより乱数を生成する回数を減らすことができる。

[0180] 群Hの任意の元hについて、 $g \in G$ で $\theta(g, h) = \nu$ となるものを計算することが困難ならば、第四実施形態と比較して安全性は低下しない。

[0181] [第九実施形態]

第九実施形態の代理計算システムは、依頼装置 1' が図 1 2 に破線で示された事前計算部 2 9' を更に含み、ステップS 1 1 5' が第四実施形態の代理計算システムとは異なり、他の部分については第四実施形態の代理計算システムと同様である。以下、第四実施形態と異なる部分を中心に説明する。

[0182] 事前計算部 2 9' は、第三乱数生成部 2 7' が生成した d_1 を用いて g^{d_1} を計算する。この処理は、ステップS 1 1 2' の後、ステップS 1 1 5' の前に行う。

第三入力情報計算部 2 3' は、事前計算された g^{d_1} を用いて、 $g_2 = \mu_g^{r_4} g^{d_1}$ の計算を行う（ステップS 1 1 5' ）。

[0183] ステップS 1 1 4' で、判定条件を満たさない場合にはステップS 1 1' からステップS 1 2 3' の処理が繰り返されるが、この繰り返しの処理においては、事前計算された g^{d_1} を再利用する。すなわち、第三乱数生成部 2 7' は乱数 d_1 を生成せず、第三入力情報計算部 2 3' は事前計算された g^{d_1} を用いて、 $g_2 = \mu_g^{r_4} g^{d_1}$ の計算を行う。これにより、乱数 d_1 を生成する回数を減らすことができ、 $g_2 = \mu_g^{r_4} g^{d_1}$ の計算を速く行うことができる。

[0184] [第十実施形態]

第十実施形態の代理計算システムは、依頼装置 1' が図 1 3 に破線で示された事前計算部 4 9' を更に含み、ステップS 2 1 6' が第四実施形態の代

理計算システムとは異なり、他の部分については第四実施形態の代理計算システムと同様である。以下、第四実施形態と異なる部分を中心に説明する。

[0185] 事前計算部 4 9' は、第八乱数生成部 4 7' が生成した d_2 を用いて h^{d_2} を計算する。この処理は、ステップ S 2 1 2' の後、ステップ S 2 1 6' の前に行う。

第八入力情報計算部 4 4' は、事前計算された h^{d_2} を用いて、第八入力情報 $h_4 = \mu_{h^{r^{10\sigma}}} h^{d_2}$ の計算を行う（ステップ S 1 1 6'）。

[0186] ステップ S 2 1 4' で、判定条件を満たさない場合にはステップ S 2 1' からステップ S 2 2 3' の処理が繰り返されるが、この繰り返しの処理においては、事前計算された h^{d_2} を再利用する。すなわち、第八乱数生成部 4 7' は乱数 d_2 を生成せず、第八入力情報計算部 4 4' は事前計算された h^{d_2} を用いて、 $h_4 = \mu_{h^{r^{10\sigma}}} h^{d_2}$ の計算を行う。これにより、乱数 d_2 を生成する回数を減らすことができ、 $h_4 = \mu_{h^{r^{10\sigma}}} h^{d_2}$ の計算を速く行うことができる。

[0187] [第四実施形態から第十実施形態の変形例等]

第一乱数生成部 1 1'、第二乱数生成部 1 2'、第三乱数生成部 2 7'、第四乱数生成部 2 1'、第五乱数生成部 2 2'、第六乱数生成部 3 1'、第七乱数生成部 3 2'、第八乱数生成部 4 7'、第九乱数生成部 4 1' 及び第十乱数生成部 4 2' のそれぞれは、一様乱数を生成することにより、代理計算システムの安全性が最も高くなる。しかし、求める安全性のレベルがそれほど高くない場合には、第一乱数生成部 1 1'、第二乱数生成部 1 2'、第三乱数生成部 2 7'、第四乱数生成部 2 1'、第五乱数生成部 2 2'、第六乱数生成部 3 1'、第七乱数生成部 3 2'、第八乱数生成部 4 7'、第九乱数生成部 4 1' 及び第十乱数生成部 4 2' のそれぞれは、一様乱数ではない乱数を生成してもよい。

[0188] リスト L_1 、リスト L_2 に情報の組が追加される毎に、第一判定部 2 8' の処理を行ってもよい。例えば、第二リスト記憶部 2 6' に情報の組 ($d_1, r_5, z_2 \nu^{-r_4 r_5}$) が記憶されている場合には、ステップ S 1 1 1' の後に、

ステップS 1 2 4' の処理を行っても良い。同様に、リスト L_3 、リスト L_4 に情報の組が追加される毎に、第二判定部 4 8' の処理を行ってもよい。

[0189] 第四実施形態から第十実施形態は互いに組み合わせることができる。

[0190] 依頼装置 1' の各部間のデータのやり取りは直接行われてもよいし、図示していない記憶部を介して行われてもよい。同様に、計算装置 2' の各部間のデータのやり取りは直接行われてもよいし、図示していない記憶部を介して行われてもよい。

[0191] 依頼装置 1' 及び計算装置 2' のそれぞれはコンピュータによって実現することができる。この場合、この装置が有すべき各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、これ装置における各処理機能が、コンピュータ上で実現される。

[0192] 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。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、これらの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。

[0193] なお、第一実施形態から第三実施形態と、第四実施形態から第十実施形態とを組み合わせてもよい。例えば、図 1 7 に例示するように、第一実施形態から第三実施形態の計算装置 2 が第四実施形態から第十実施形態の依頼装置 1' を備えており、この依頼装置 1' を含む計算装置 2 が、第四実施形態から第十実施形態で説明したのと同様にして計算装置 2' を用いて、関数 f の計算を行ってもよい。

[0194] 具体的には、計算装置 2 は計算する必要がある関数 $f(x)$ を計算するために、対応する写像 $\theta(g, h)$ の値を、計算装置 2' を用いて計算する。関数 $f(x)$ に対応する写像 $\theta(g, h)$ とは、与えられた関数 f 及び x に対して、関数 $f(x)$ と値が同じ値を出力する写像 $\theta(g, h)$ である。ある元 $h \in H$ に関して、 $f(x) = \theta(x, h)$ という関係がある場合には、

$f(x)$ に対応する写像 θ が $\theta(x, h)$ となる。

[0195] 例えば、参考文献1に記載されたBoneh-Franklin方式のIDベース暗号において、ある一定のIDに関する復号関数を f とする。この方式のIDベース暗号では、楕円曲線の点がなす有限群 G, H と、ペアリング $\tau: G \times H \rightarrow F$ を用いて構成される。 Q を G の元とする。IDベース暗号の鍵発行センタの秘密鍵を s として、公開鍵を $P = sQ$ とする。IDベース暗号のパブリックパラメータは、群 G, H の記述と、ペアリング τ の記述、 Q 及び P である。

[0196] [参考文献1] Dan Boneh, Matt Franklin, "Identity-Based Encryption from the Weil Pairing", CRYPTO 2001, LNCS 2139, pp.213-229, 2001.

鍵の発行は以下のようにして行われる。鍵発行センタは、IDに対応して定まる H の元 Q_{ID} について、 $P_{ID} = sQ_{ID}$ を計算してIDの保持者に対して通知する。 P_{ID} はIDの保持者の秘密鍵である。このとき、復号関数 $f: G \rightarrow F$ は、 $f(x) = \tau(x, P_{ID})$ で定義される。

[0197] 暗号文の作成、暗号文の復号は以下のようにして行われる。平文 m をあるIDについて暗号化するためには、乱数 r を生成して $(Q^r, m \oplus H(\tau(P^r, Q_{ID})))$ を計算し、これを暗号文 (C_1, C_2) とする。復号するためには、暗号文 (C_1, C_2) に対して、 $C_2 \oplus H(f(C_1))$ を計算することで平文が得られる。ただし、ここで H はハッシュ関数、 $(\oplus)$ は排他的論理和である。

[0198] このようなBoneh-Franklin方式のIDベース暗号において、関数 $f(x)$ に対応する写像 θ は例えばペアリング τ を用いて定義される。すなわち、 $f(x) = \tau(x, P_{ID})$ である。

[0199] 計算装置2がICカードや携帯電話であり、秘密情報の抽出が困難であるが、計算能力が限定されている場合に、このように依頼装置及び計算装置を多重にして組み合わせることが有益である。

[0200] この発明は、上述の実施形態に限定されるものではなく、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。

請求の範囲

[請求項1] G , H を巡回群、 f を群 H の元 x を群 G へ写す関数、 X_1 , X_2 を群 G に値を持つ確率変数、確率変数 X_1 の実現値を x_1 、確率変数 X_2 の実現値を x_2 として、

互いに素である2つの自然数 a , b を用いて、 $a' a + b' b = 1$ の関係を満たす整数 a' , b' を計算する整数計算部と、

$f(x)^b x_1$ を計算可能であり、その計算結果を u とする第一乱数化可能標本器と、

$u' = u^a$ を計算する第一べき乗計算部と、

$f(x)^a x_2$ を計算可能であり、その計算結果を v とする第二乱数化可能標本器と、

$v' = v^b$ を計算する第二べき乗計算部と、

$u' = v'$ であるか判定する判定部と、

$u' = v'$ であると判定された場合には、 $u^{b'} v^{a'}$ を計算する最終計算部と、

を含む代理計算システム。

[請求項2] 請求項1の代理計算システムにおいて、

X_3 を群 G に値を持つ確率変数、確率変数 X_3 の実現値を x_3 として、 $f(x) x_3$ を計算可能であり、 $a = 1$ であれば上記第二乱数化可能標本器に代わりその計算結果を上記 v とし、 $b = 1$ であれば上記第一乱数化可能標本器に代わりその計算結果を上記 u とする標本器を更に含む、

代理計算システム。

[請求項3] 請求項1の代理計算システムにおいて、

上記 f を準同型写像、群 H の生成元を μ_h 、群 H の位数を K_H 、 $\nu = f(\mu_h)$ として、

上記第一乱数化可能標本器は、0以上 K_H 未満の整数の乱数 r_1 を生成する第一乱数生成部と、第一入力情報 $\mu_h^{r_1} x^b$ を計算する第一

入力情報計算部と、上記第一入力情報 $\mu_h^{r_1} \times b$ を用いて $f(\mu_h^{r_1} \times b)$ を計算可能でありその計算結果を第一出力情報 z_1 とする第一出力情報計算部と、 $z_1 \nu^{-r_1}$ を計算してその計算結果を上記 u とする第一計算部とを含み、

上記第二乱数化可能標本器は、0 以上 K_H 未満の整数の乱数 r_2 を生成する第二乱数生成部と、第二入力情報 $\mu_h^{r_2} \times a$ を計算する第二入力情報計算部と、上記第二入力情報 $\mu_h^{r_2} \times a$ を用いて $f(\mu_h^{r_2} \times a)$ を計算可能でありその計算結果を第二出力情報 z_2 とする第二出力情報計算部と、 $z_2 \nu^{-r_2}$ を計算してその計算結果を上記 v とする第二計算部とを含む、

代理計算システム。

[請求項4] 請求項3の代理計算システムにおいて、

0 以上 K_H 未満の整数の乱数 r_3 を生成する第三乱数生成部と、第三入力情報 x^{r_3} を計算する第三入力情報計算部と、上記第三入力情報 x^{r_3} を用いて $f(x^{r_3})$ を計算可能でありその計算結果を第三出力情報 z_3 とする第三出力情報計算部と、 z_3^{1/r_3} を計算して $a = 1$ あれば上記第二乱数化可能標本器に代わりその計算結果を上記 v とし $b = 1$ であれば上記第一乱数化可能標本器に代わりその計算結果を上記 u とする第三計算部とを含む標本器を更に含む、

代理計算システム。

[請求項5] 請求項1の代理計算システムにおいて、

群 $H = G \times G$ 、上記 f を準同型写像、群 G の生成元を μ_g 、群 G の位数を K_G 、 $x = (c_1, c_2)$ 、 (V, W) を群 H の元、 $f(V, W) = Y$ として、

上記第一乱数化可能標本器は、0 以上 K_G 未満の整数の乱数 r_4 を生成する第四乱数生成部と、0 以上 K_G 未満の整数の乱数 r_5 を生成する第五乱数生成部と、第四入力情報 $c_1^b V^{r_4} \mu_g^{r_5}$ を計算する第四入力情報計算部と、第五入力情報 $c_2^b W^{r_4}$ を計算する第五入力情報

計算部と、上記第四入力情報 $c_1^b V^{r_4} \mu_g^{r_5}$ 及び上記第五入力情報 $c_2^b W^{r_4}$ を用いて $f(c_1^b V^{r_4} \mu_g^{r_5}, c_2^b W^{r_4})$ を計算可能でありその計算結果を第四出力情報 z_4 とする第四出力情報計算部と、 $z_4 Y^{-r_4} \mu_g^{-r_5}$ を計算してその計算結果を上記 u とする第四計算部とを含み、

上記第二乱数化可能標本器は、0 以上 K_G 未満の整数の乱数 r_6 を生成する第六乱数生成部と、0 以上 K_G 未満の整数の乱数 r_7 を生成する第七乱数生成部と、第六入力情報 $c_1^a V^{r_6} \mu_g^{r_7}$ を計算する第六入力情報計算部と、第七入力情報 $c_2^a W^{r_6}$ を計算する第七入力情報計算部と、上記第六入力情報 $c_1^a V^{r_6} \mu_g^{r_7}$ 及び上記第七入力情報 $c_2^a W^{r_6}$ を用いて $f(c_1^a V^{r_6} \mu_g^{r_7}, c_2^a W^{r_6})$ を計算可能でありその計算結果を第五出力情報 z_5 とする第五出力情報計算部と、 $z_5 Y^{-r_6} \mu_g^{-r_7}$ を計算してその計算結果を上記 v とする第五計算部とを含む、

代理計算システム。

[請求項6]

G , H を巡回群、 f を群 H の元 x を群 G へ写す関数、 X_1 , X_2 を群 G に値を持つ確率変数、確率変数 X_1 の実現値を x_1 、確率変数 X_2 の実現値を x_2 として、

整数計算部が、互いに素である2つの自然数 a , b を用いて、 a' , $a + b'$, $b = 1$ の関係を満たす整数 a' , b' を計算する整数計算ステップと、

第一乱数化可能標本器が、 $f(x)^b x_1$ を計算可能であり、その計算結果を u とする第一乱数化可能標本抽出ステップと、

第一べき乗計算部が、 $u' = u^a$ を計算する第一べき乗計算ステップと、

第二乱数化可能標本器が、 $f(x)^a x_2$ を計算可能であり、その計算結果を v とする第二乱数化可能標本抽出ステップと、

第二べき乗計算部が、 $v' = v^b$ を計算する第二べき乗計算ステッ

プと、

判定部が、 $u' = v'$ であるか判定する判定ステップと、

最終計算部が、 $u' = v'$ であると判定された場合には、 $u^{b'} v^{a'}$

を計算する最終計算ステップと、

を含む代理計算方法。

[請求項7]

G 、 H を巡回群、 f を群 H の元 x を群 G へ写す関数、 X_1 、 X_2 を群 G に値を持つ確率変数、確率変数 X_1 の実現値を x_1 、確率変数 X_2 の実現値を x_2 として、

互いに素である2つの自然数 a 、 b を用いて、 $a' a + b' b = 1$ の関係を満たす整数 a' 、 b' を計算する整数計算部と、

$f(x)^{b'} x_1$ を計算可能な第一乱数化可能標本器による計算結果 u を用いて $u' = u^{a'}$ を計算する第一べき乗計算部と、

$f(x)^{a'} x_2$ を計算可能な第二乱数化可能標本器による計算結果 v を用いて $v' = v^{b'}$ を計算する第二べき乗計算部と、

$u' = v'$ であるか判定する判定部と、

$u' = v'$ であると判定された場合には、 $u^{b'} v^{a'}$ を計算する最終計算部と、

を含む依頼装置。

[請求項8]

依頼装置が計算装置に依頼した計算の結果を用いて $\theta(g, h)$ を計算する代理計算システムにおいて、

G 、 H 及び F を巡回群とし、写像 $\theta : G \times H \rightarrow F$ を双準同型写像とし、 g を群 G の元とし、 h を群 H の元とし、 K_G を群 G の位数とし、 K_H を群 H の位数とし、 μ_g を群 G の生成元とし、 μ_h を群 H の生成元とし、 $\nu = \theta(\mu_g, \mu_h)$ とし、 k を自然数のセキュリティパラメータとし、 $K = 2^k$ として、

上記依頼装置は、

0以上 K_G 未満の整数の乱数 r_1 を生成する第一乱数生成部と、

0以上 K_H 未満の整数の乱数 r_2 を生成する第二乱数生成部と、

第一入力情報 $g_1 = \mu_g r^1 g$ を計算する第一入力情報計算部と、

第二入力情報 $h_1 = \mu_h r^2$ を計算する第二入力情報計算部と、

上記計算装置から受信した $z_1 \in F$ を用いて、 $z_1 \nu^{-r^1 r^2}$ を計算する第一リスト情報計算部と、

上記乱数 r_2 と上記計算された $z_1 \nu^{-r^1 r^2}$ とから構成される情報の組 $(r_2, z_1 \nu^{-r^1 r^2})$ が記憶される第一リスト記憶部と、

0 以上 K 未満の整数の一樣乱数である d_1 を生成する第三乱数生成部と、

0 以上 K_G 未満の整数の一樣乱数である r_4 を生成する第四乱数生成部と、

0 以上 K_H 未満の整数の一樣乱数である r_5 を生成する第五乱数生成部と、

第三入力情報 $g_2 = \mu_g r^4 g^{d_1}$ を計算する第三入力情報計算部と、

第四入力情報 $h_2 = \mu_h r^5$ を計算する第四入力情報計算部と、

上記計算装置から受信した $z_2 \in F$ を用いて、 $z_2 \nu^{-r^4 r^5}$ を計算する第二リスト情報計算部と、

上記 d_1 と上記 r_5 と上記計算された $z_2 \nu^{-r^4 r^5}$ とから構成される情報の組 $(d_1, r_5, z_2 \nu^{-r^4 r^5})$ が記憶される第二リスト記憶部と、

上記第一リスト記憶部から読み込んだ情報の組の第一成分を s_1 とし、第二成分を w_1 とし、上記第二リスト記憶部から読み込んだ情報の組の第一成分を t_2 とし、第二成分を s_2 とし、第三成分を w_2 とし、これらの情報の組が $(w_1)^{\wedge} (t_2 s_2 s_1^{-1}) = w_2$ の関係を満たすかを判定し、その関係を満たす場合には、 s_1 を σ に代入し、 w_1 を ν' に代入する第一判定部と、

0 以上 K_G 未満の整数の一樣乱数である r_6 を生成する第六乱数生成部と、

0 以上 K_H 未満の整数の一樣乱数である r_7 を生成する第七乱数生

成部と、

第五入力情報 $g_3 = g^{r_6}$ を計算する第五入力情報計算部と、

第六入力情報 $h_3 = \mu_h^{r_7 \sigma} h$ を計算する第六入力情報計算部と、

上記計算装置から受信した $z_3 \in F$ を用いて、 $z_3 \nu'^{-r_6 r_7}$ を計算する第三リスト情報計算部と、

上記 r_6 と上記計算された $z_3 \nu'^{-r_6 r_7}$ とから構成される情報の組 $(r_6, z_3 \nu'^{-r_6 r_7})$ が記憶される第三リスト記憶部と、

0 以上 K 未満の整数の一樣乱数である d_2 を生成する第八乱数生成部と、

0 以上 K_G 未満の整数の一樣乱数である r_9 を生成する第九乱数生成部と、

0 以上 K_H 未満の整数の一樣乱数である r_{10} を生成する第十乱数生成部と、

第七入力情報 $g_4 = \mu_g^{r_9}$ を計算する第七入力情報計算部と、

第八入力情報 $h_4 = \mu_h^{r_{10} \sigma} h^{d_2}$ を計算する第八入力情報計算部と

、

上記計算装置から受信した $z_4 \in F$ を用いて、 $z_4 \nu'^{-r_9 r_{10}}$ を計算する第四リスト情報計算部と、

上記 d_2 と上記 r_9 と上記計算された $z_4 \nu'^{-r_9 r_{10}}$ とから構成される情報の組 $(d_2, r_9, z_4 \nu'^{-r_9 r_{10}})$ が記憶される第四リスト記憶部と、

上記第三リスト記憶部から読み込んだ情報の組の第一成分を s_3 とし、第二成分を w_3 とし、上記第四リスト記憶部から読み込んだ情報の組の第一成分を t_4 とし、第二成分を s_4 とし、第三成分を w_4 とし、これらの情報の組が $(w_3)^{\wedge} (t_4 s_4 s_3^{-1}) = w_4$ の関係を満たすかを判定し、その関係を満たす場合には、 $(w_3)^{\wedge} (s_3^{-1})$ を出力する第二判定部と、

を含み、

上記計算装置は、

上記依頼装置から受信した g_1 及び h_1 を用いて $\theta(g_1, h_1)$ を計算可能であり、その計算結果を上記 z_1 として出力する第一出力情報計算部と、

上記依頼装置から受信した g_2 及び h_2 を用いて $\theta(g_2, h_2)$ を計算可能であり、その計算結果を上記 z_2 として出力する第二出力情報計算部と、

上記依頼装置から受信した g_3 及び h_3 を用いて $\theta(g_3, h_3)$ を計算可能であり、その計算結果を上記 z_3 として出力する第三出力情報計算部と、

上記依頼装置から受信した g_4 及び h_4 を用いて $\theta(g_4, h_4)$ を計算可能であり、その計算結果を上記 z_4 として出力する第四出力情報計算部と、

を含む、

代理計算システム。

[請求項9]

請求項8の代理計算システムにおいて、

上記第一入力情報計算部は、第一入力情報 $g_1 = g^{r_1}$ を計算し、

上記第一リスト情報計算部は、上記 r_1 及び上記 r_2 を用いて $r_1 r_2$ を計算し、

上記第一リスト記憶部には、上記計算された $r_1 r_2$ と上記計算装置から受信した $z_1 \in F$ とから構成される情報の組 $(r_1 r_2, z_1)$ が記憶される、

ことを特徴とする代理計算システム。

[請求項10]

請求項8又は9に記載の代理計算システムにおいて、

上記第六入力情報計算部は、第六入力情報 $h_3 = h^{r_7}$ を計算し、

上記第三リスト情報計算部は、上記 r_6 及び上記 r_7 を用いて $r_6 r_7$ を計算し、

上記第三リスト記憶部には、上記計算された $r_6 r_7$ と上記計算装

置から受信した $z_3 \in F$ とから構成される情報の組 $(r_6 r_7, z_3)$ が記憶される、

ことを特徴とする代理計算システム。

[請求項11] 請求項8から10の何れかに記載の代理計算システムにおいて、
上記第一判定部は、上記の関係を満たす場合には、 $t_1 s_2$ を σ に代入し、 w_2 を ν' に代入し、
上記第十乱数生成部は、上記 r_9 を用いて $-r_9^{-1}$ を計算して r_{10} とする、

ことを特徴とする代理計算システム。

[請求項12] 請求項11に記載の代理計算システムにおいて、
上記第七乱数生成部は、上記 r_6 を用いて $-r_6^{-1}$ を計算して r_7 とし、

上記第三リスト記憶部には、1 と上記計算された $z_3 \nu' - r_6 r_7$ とから構成される情報の組 $(1, z_3 \nu' - r_6 r_7)$ が記憶される、

ことを特徴とする代理計算システム。

[請求項13] 請求項8から12の何れかに記載の代理計算システムにおいて、
上記第四乱数生成部は、上記 r_5 を用いて $-r_5^{-1}$ を計算して r_4 とする、

ことを特徴とする代理計算システム。

[請求項14] 請求項8から13の何れかに記載の代理計算システムにおいて、
上記 d_1 を用いて g^{d_1} を計算する事前計算部を更に含み、
上記第三入力情報計算部は、上記事前計算された g^{d_1} を用いて、
上記 g_2 の計算を行う、 ことを特徴とする代理計算システム。

[請求項15] 請求項8から14の何れかに記載の代理計算システムにおいて、
上記 d_2 を用いて h^{d_2} を計算する事前計算部を更に含み、
上記第八入力情報計算部は、上記事前計算された h^{d_2} を用いて、
上記 h_4 の計算を行う、

ことを特徴とする代理計算システム。

[請求項16] 依頼装置が計算装置に依頼した計算の結果を用いて $\theta(g, h)$ を計算する代理計算方法において、

G 、 H 及び F を巡回群とし、写像 $\theta : G \times H \rightarrow F$ を双準同型写像とし、 g を群 G の元とし、 h を群 H の元とし、 K_G を群 G の位数とし、 K_H を群 H の位数とし、 μ_g を群 G の生成元とし、 μ_h を群 H の生成元とし、 $\nu = \theta(\mu_g, \mu_h)$ とし、 k を整数のセキュリティパラメータとし、 $K = 2^k$ として、

上記依頼装置の第一乱数生成部が、0 以上 K_G 未満の整数の乱数 r_1 を生成する第一乱数生成ステップと、

上記依頼装置の第二乱数生成部が、0 以上 K_H 未満の整数の乱数 r_2 を生成する第二乱数生成ステップと、

上記依頼装置の第一入力情報計算部が、第一入力情報 $g_1 = \mu_g^{r_1}$ g を計算する第一入力情報計算ステップと、

上記依頼装置の第二入力情報計算部が、第二入力情報 $h_1 = \mu_h^{r_2}$ h を計算する第二入力情報計算ステップと、

上記計算装置の第一出力情報計算部が、上記依頼装置から受信した g_1 及び h_1 を用いて $\theta(g_1, h_1)$ を計算可能であり、その計算結果を上記 z_1 として出力する第一出力情報計算ステップと、

上記依頼装置の第一リスト情報計算部が、上記計算装置から受信した $z_1 \in F$ を用いて、 $z_1 \nu^{-r_1 r_2}$ を計算する第一リスト情報計算ステップと、

上記依頼装置の第一リスト記憶部に、上記乱数 r_2 と上記計算された $z_1 \nu^{-r_1 r_2}$ とから構成される情報の組 $(r_2, z_1 \nu^{-r_1 r_2})$ が記憶されるステップと、

上記依頼装置の第三乱数生成部が、0 以上 K 未満の整数の一樣乱数である d_1 を生成する第三乱数生成ステップと、

上記依頼装置の第四乱数生成部が、0 以上 K_G 未満の整数の一樣乱数である r_4 を生成する第四乱数生成ステップと、

上記依頼装置の第五乱数生成部が、0以上 K_H 未満の整数の一樣乱数である r_5 を生成する第五乱数生成ステップと、

上記依頼装置の第三入力情報計算部が、第三入力情報 $g_2 = \mu_g^{r_4} g^{d_1}$ を計算する第三入力情報計算ステップと、

上記依頼装置の第四入力情報計算部が、第四入力情報 $h_2 = \mu_h^{r_5}$ を計算する第四入力情報計算ステップと、

上記計算装置の第二出力情報計算部が、上記依頼装置から受信した g_2 及び h_2 を用いて $\theta(g_2, h_2)$ を計算可能であり、その計算結果を上記 z_2 として出力する第二出力情報計算ステップと、

上記依頼装置の第二リスト情報計算部が、上記計算装置から受信した $z_2 \in F$ を用いて、 $z_2 \nu^{-r_4 r_5}$ を計算する第二リスト情報計算ステップと、

上記依頼装置の第二リスト記憶部に、上記 d_1 と上記 r_5 と上記計算された $z_2 \nu^{-r_4 r_5}$ とから構成される情報の組 $(d_1, r_5, z_2 \nu^{-r_4 r_5})$ が記憶されるステップと、

上記依頼装置の第一判定部が、上記第一リスト記憶部から読み込んだ情報の組の第一成分を s_1 とし、第二成分を w_1 とし、上記第二リスト記憶部から読み込んだ情報の組の第一成分を t_2 とし、第二成分を s_2 とし、第三成分を w_2 として、これらの情報の組が $(w_1)^\wedge (t_2 s_2 s_1^{-1}) = w_2$ の関係を満たすかを判定し、その関係を満たす場合には、 s_1 を σ に代入し、 w_1 を ν' に代入する第一判定ステップと、

上記依頼装置の第六乱数生成部が、0以上 K_G 未満の整数の一樣乱数である r_6 を生成する第六乱数生成ステップと、

上記依頼装置の第七乱数生成部が、0以上 K_H 未満の整数の一樣乱数である r_7 を生成する第七乱数生成ステップと、

上記依頼装置の第五入力情報計算部が、第五入力情報 $g_3 = g^{r_6}$ を計算する第五入力情報計算ステップと、

上記依頼装置の第六入力情報計算部が、第六入力情報 $h_3 = \mu_h r^{7\sigma}$ h を計算する第六入力情報計算ステップと、

上記計算装置の第三出力情報計算部が、上記依頼装置から受信した g_3 及び h_3 を用いて $\theta(g_3, h_3)$ を計算可能であり、その計算結果を上記 z_3 として出力する第三出力情報計算ステップと、

上記依頼装置の第三リスト情報計算部が、上記計算装置から受信した $z_3 \in F$ を用いて、 $z_3 \nu' - r_6 r^7$ を計算する第三リスト情報計算ステップと、

上記依頼装置の第三リスト記憶部に、上記 r_6 と上記計算された $z_3 \nu' - r_6 r^7$ とから構成される情報の組 $(r_6, z_3 \nu' - r_6 r^7)$ が記憶されるステップと、

上記依頼装置の第八乱数生成部が、0以上K未満の整数の一樣乱数である d_2 を生成する第八乱数生成ステップと、

上記依頼装置の第九乱数生成部が、0以上 K_g 未満の整数の一樣乱数である r_9 を生成する第九乱数生成ステップと、

上記依頼装置の第十乱数生成部が、0以上 K_h 未満の整数の一樣乱数である r_{10} を生成する第十乱数生成ステップと、

上記依頼装置の第七入力情報計算部が、第七入力情報 $g_4 = \mu_g r^9$ を計算する第七入力情報計算ステップと、

上記依頼装置の第八入力情報計算部が、第八入力情報 $h_4 = \mu_h r^{10\sigma} h^{d_2}$ を計算する第八入力情報計算ステップと、

上記計算装置の第四出力情報計算部が、上記依頼装置から受信した g_4 及び h_4 を用いて $\theta(g_4, h_4)$ を計算可能であり、その計算結果を上記 z_4 として出力する第四出力情報計算ステップと、

上記依頼装置の第四リスト情報計算部が、上記計算装置から受信した $z_4 \in F$ を用いて、 $z_4 \nu' - r_9 r^{10}$ を計算する第四リスト情報計算ステップと、

上記依頼装置の第四リスト記憶部に、上記 d_2 と上記 r_9 と上記計

算された $z_4 \nu^{-r_9 r_{10}}$ とから構成される情報の組 $(d_2, r_9, z_4 \nu^{-r_9 r_{10}})$ が記憶されるステップと、

上記依頼装置の第二判定部が、上記第三リスト記憶部から読み込んだ情報の組の第一成分を s_3 とし、第二成分を w_3 とし、上記第四リスト記憶部から読み込んだ情報の組の第一成分を t_4 とし、第二成分を s_4 とし、第三成分を w_4 として、これらの情報の組が $(w_3)^{\wedge} (t_4 s_4 s_3^{-1}) = w_4$ の関係を満たすかを判定し、その関係を満たす場合には、 $(w_3)^{\wedge} (s_3^{-1})$ を出力する第二判定ステップと、
を含む代理計算方法。

[請求項17] 依頼装置が計算装置に依頼した計算の結果を用いて $\theta(g, h)$ を計算する代理計算システムの依頼装置において、

G 、 H 及び F を巡回群とし、写像 $\theta : G \times H \rightarrow F$ を双準同型写像とし、 g を群 G の元とし、 h を群 H の元とし、 K_G を群 G の位数とし、 K_H を群 H の位数とし、 μ_g を群 G の生成元とし、 μ_h を群 H の生成元とし、 $\nu = \theta(\mu_g, \mu_h)$ とし、 k を自然数のセキュリティパラメータとし、 $K = 2^k$ として、

0 以上 K_G 未満の整数の乱数 r_1 を生成する第一乱数生成部と、

0 以上 K_H 未満の整数の乱数 r_2 を生成する第二乱数生成部と、

第一入力情報 $g_1 = \mu_g^{r_1} g$ を計算する第一入力情報計算部と、

第二入力情報 $h_1 = \mu_h^{r_2}$ を計算する第二入力情報計算部と、

上記計算装置から受信した $z_1 \in F$ を用いて、 $z_1 \nu^{-r_1 r_2}$ を計算する第一リスト情報計算部と、

上記乱数 r_2 と上記計算された $z_1 \nu^{-r_1 r_2}$ とから構成される情報の組 $(r_2, z_1 \nu^{-r_1 r_2})$ が記憶される第一リスト記憶部と、

0 以上 K 未満の整数の一様乱数である d_1 を生成する第三乱数生成部と、

0 以上 K_G 未満の整数の一様乱数である r_4 を生成する第四乱数生成部と、

0以上 K_H 未満の整数の一樣乱数である r_5 を生成する第五乱数生成部と、

第三入力情報 $g_2 = \mu_g r_4 g^{d_1}$ を計算する第三入力情報計算部と、

第四入力情報 $h_2 = \mu_h r_5$ を計算する第四入力情報計算部と、

上記計算装置から受信した $z_2 \in F$ を用いて、 $z_2 \nu^{-r_4 r_5}$ を計算する第二リスト情報計算部と、

上記 d_1 と上記 r_5 と上記計算された $z_2 \nu^{-r_4 r_5}$ とから構成される情報の組 $(d_1, r_5, z_2 \nu^{-r_4 r_5})$ が記憶される第二リスト記憶部と、

上記第一リスト記憶部から読み込んだ情報の組の第一成分を s_1 とし、第二成分を w_1 とし、上記第二リスト記憶部から読み込んだ情報の組の第一成分を t_2 とし、第二成分を s_2 とし、第三成分を w_2 として、これらの情報の組が $(w_1)^{\wedge} (t_2 s_2 s_1^{-1}) = w_2$ の関係を満たすかを判定し、その関係を満たす場合には、 s_1 を σ に代入し、 w_1 を ν' に代入する第一判定部と、

0以上 K_G 未満の整数の一樣乱数である r_6 を生成する第六乱数生成部と、

0以上 K_H 未満の整数の一樣乱数である r_7 を生成する第七乱数生成部と、

第五入力情報 $g_3 = g^{r_6}$ を計算する第五入力情報計算部と、

第六入力情報 $h_3 = \mu_h r_7^{\sigma} h$ を計算する第六入力情報計算部と、

上記計算装置から受信した $z_3 \in F$ を用いて、 $z_3 \nu'^{-r_6 r_7}$ を計算する第三リスト情報計算部と、

上記 r_6 と上記計算された $z_3 \nu'^{-r_6 r_7}$ とから構成される情報の組 $(r_6, z_3 \nu'^{-r_6 r_7})$ が記憶される第三リスト記憶部と、

0以上 K 未満の整数の一樣乱数である d_2 を生成する第八乱数生成部と、

0以上 K_G 未満の整数の一樣乱数である r_9 を生成する第九乱数生

成部と、

0以上 K_H 未満の整数の一様乱数である r_{10} を生成する第10乱数生成部と、

第七入力情報 $g_4 = \mu_g r^9$ を計算する第七入力情報計算部と、

第八入力情報 $h_4 = \mu_h r^{10\sigma} h^{d2}$ を計算する第八入力情報計算部と

、

上記計算装置から受信した $z_4 \in F$ を用いて、 $z_4 \nu' - r^9 r^{10}$ を計算する第四リスト情報計算部と、

上記 d_2 と上記 r_9 と上記計算された $z_4 \nu' - r^9 r^{10}$ とから構成される情報の組 $(d_2, r_9, z_4 \nu' - r^9 r^{10})$ が記憶される第四リスト記憶部と、

上記第三リスト記憶部から読み込んだ情報の組の第一成分を s_3 とし、第二成分を w_3 とし、上記第四リスト記憶部から読み込んだ情報の組の第一成分を t_4 とし、第二成分を s_4 とし、第三成分を w_4 として、これらの情報の組が $(w_3)^\wedge (t_4 s_4 s_3^{-1}) = w_4$ の関係を満たすかを判定し、その関係を満たす場合には、 $(w_3)^\wedge (s_3^{-1})$ を出力する第二判定部と、

を含む依頼装置。

[請求項18] 請求項7又は請求項17の依頼装置の各部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19] 請求項18の依頼装置プログラムが記録されたコンピュータ読み取り可能な記録媒体。

[図1]

代理計算システム

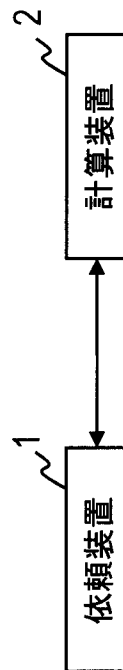


図1

[図2]

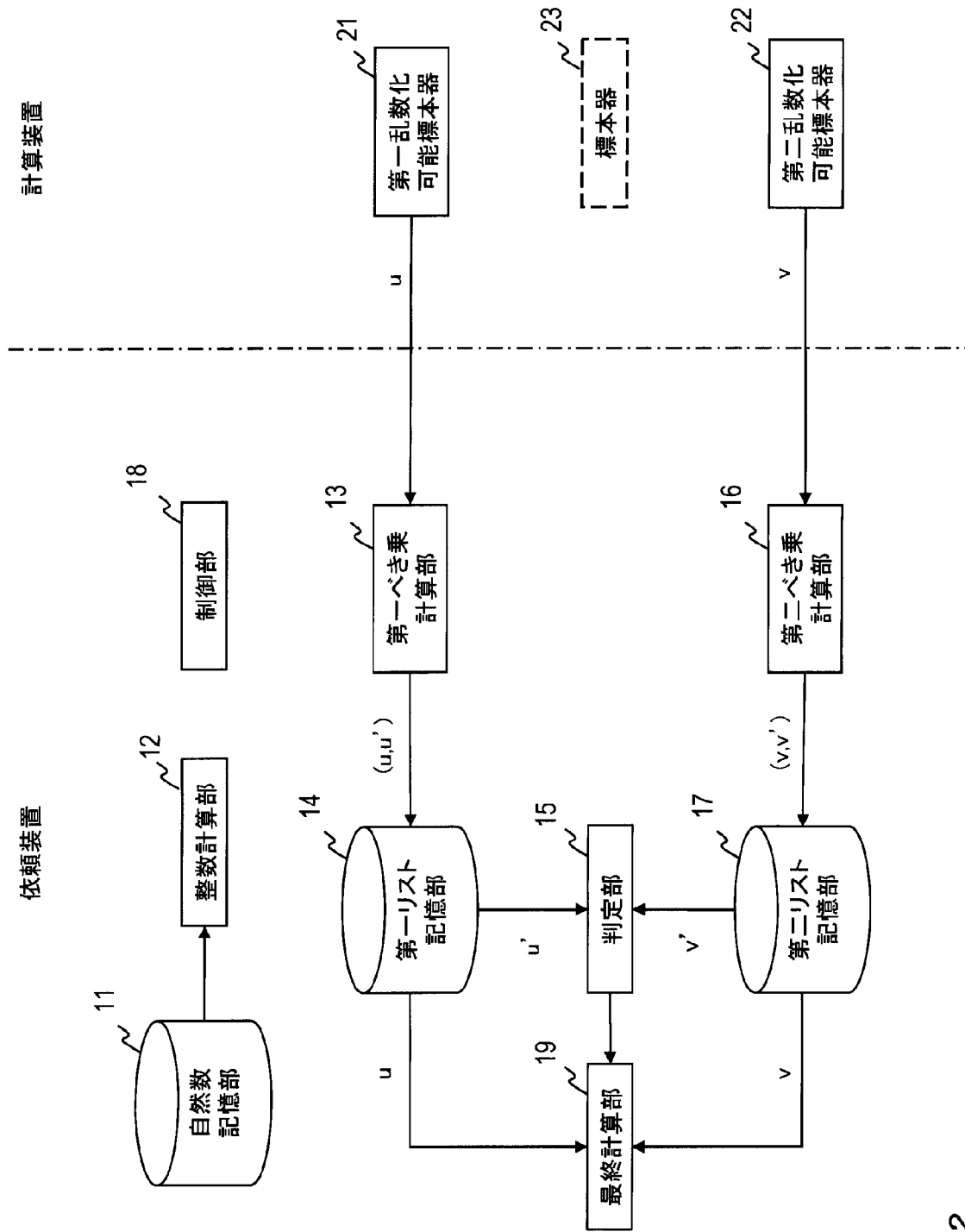


図2

[図3]

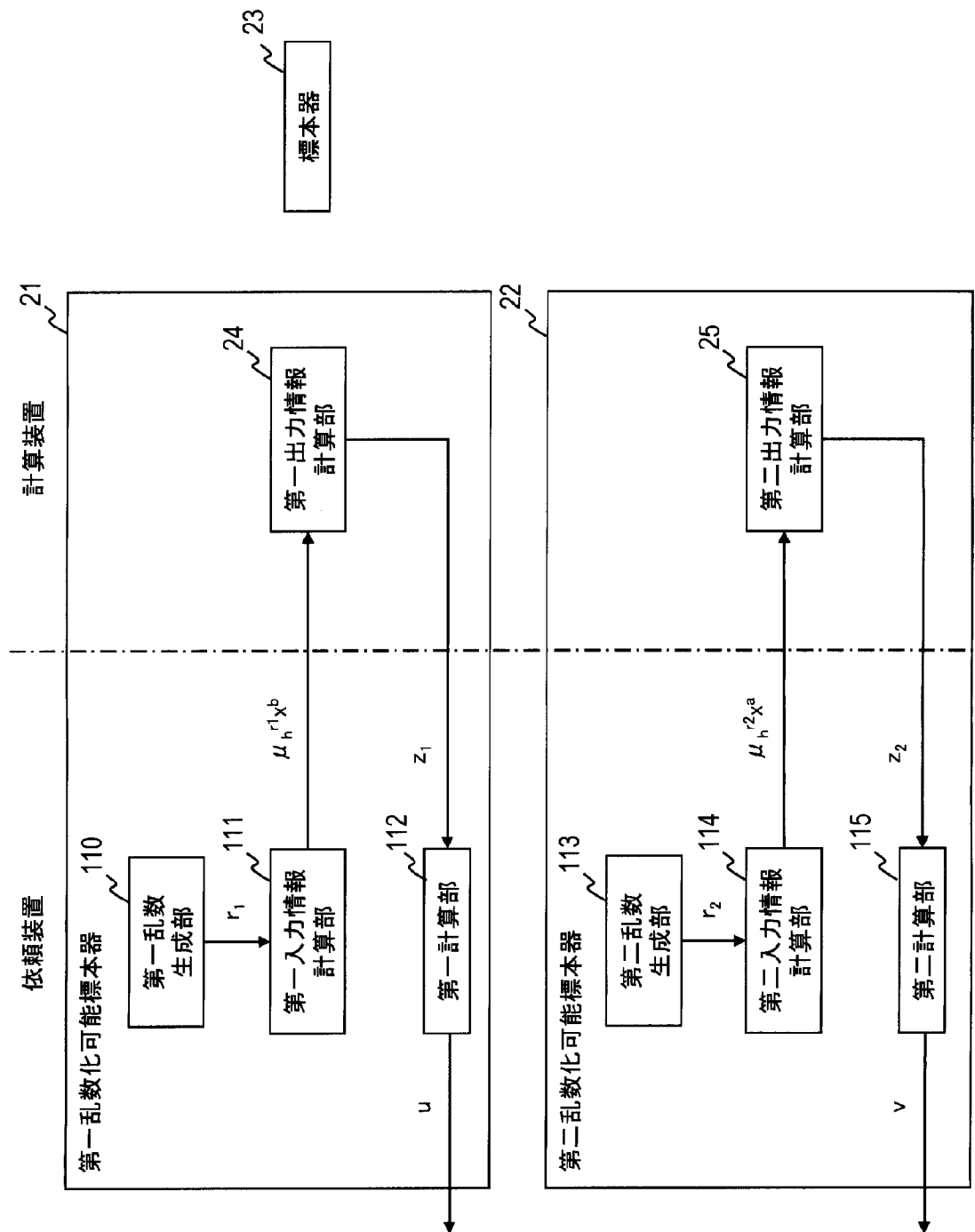


図3

[図4]

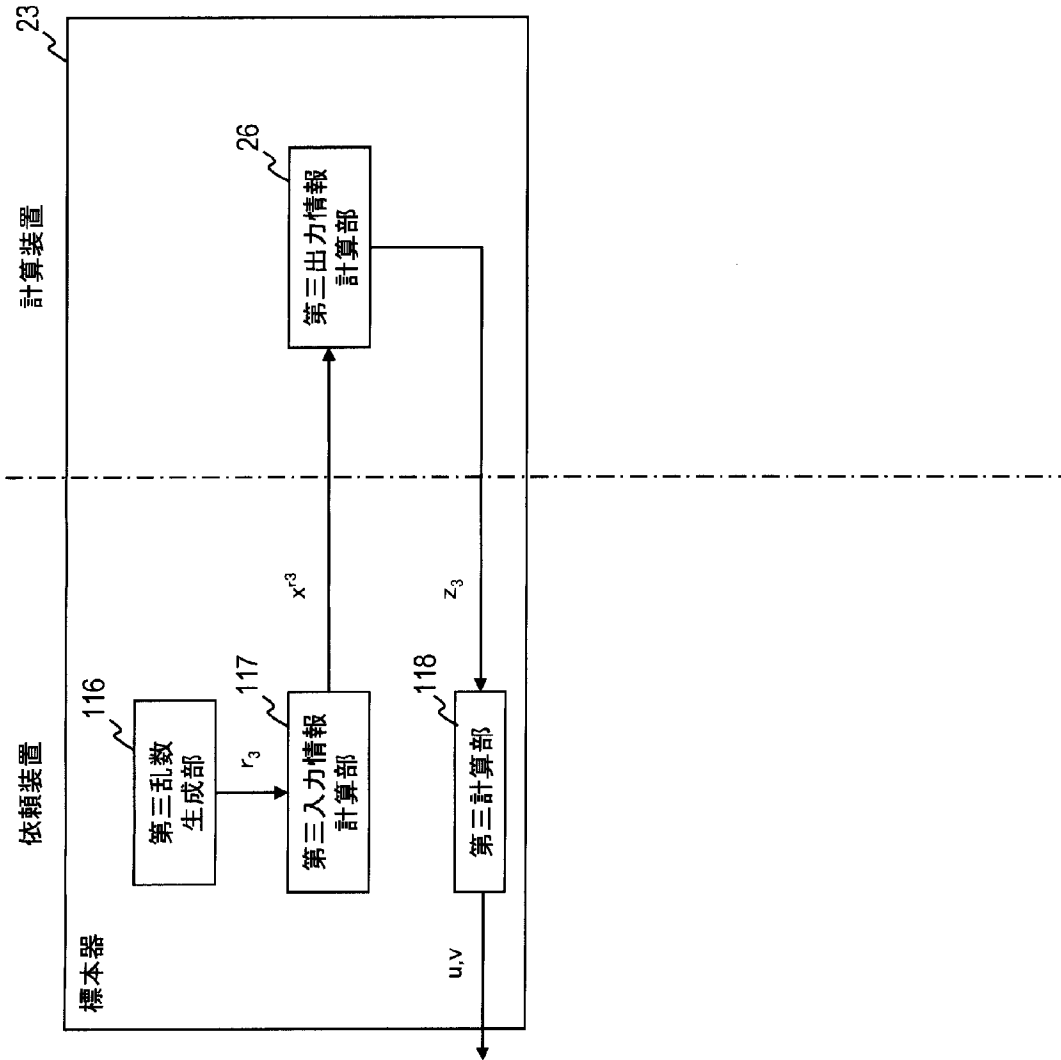


図4

[図5]

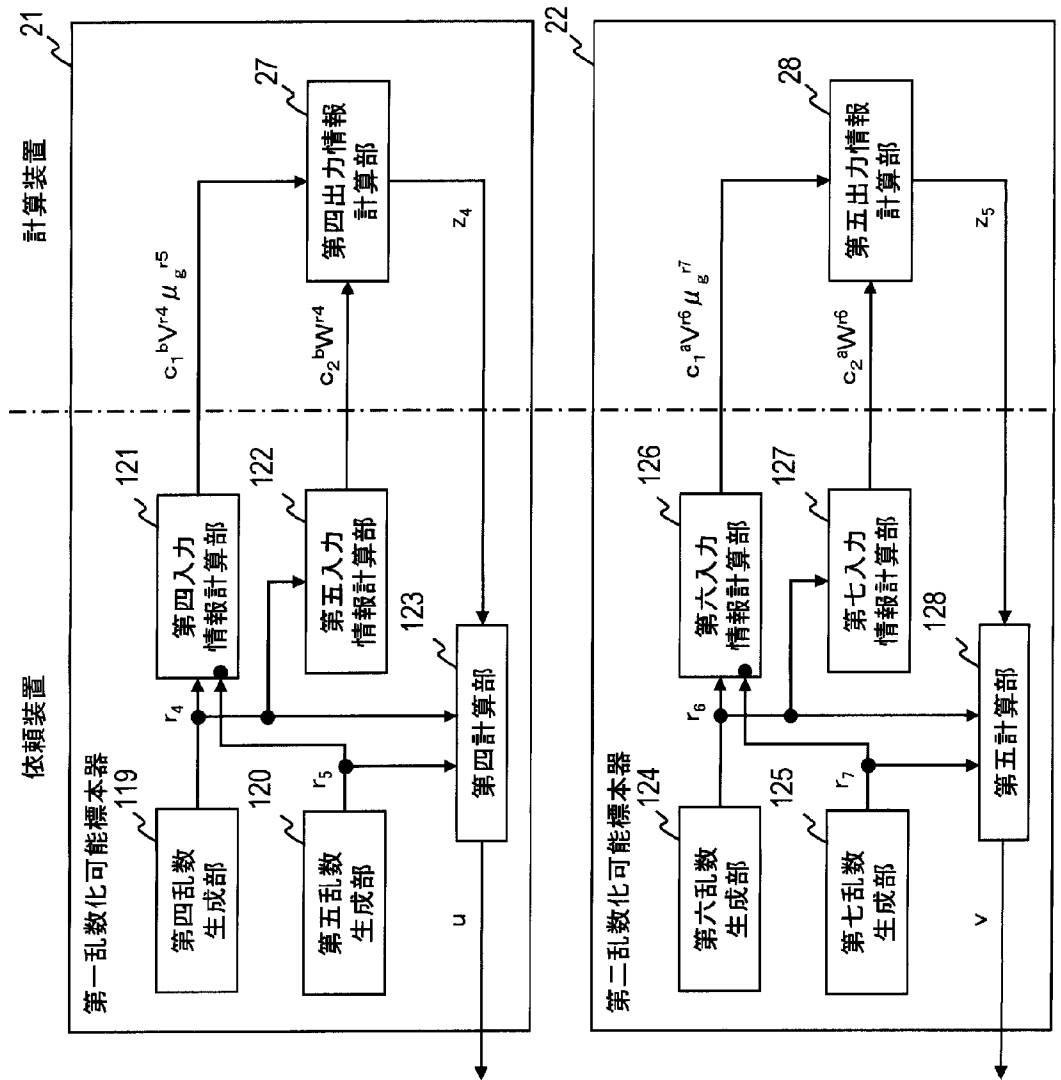


図5

[図6]

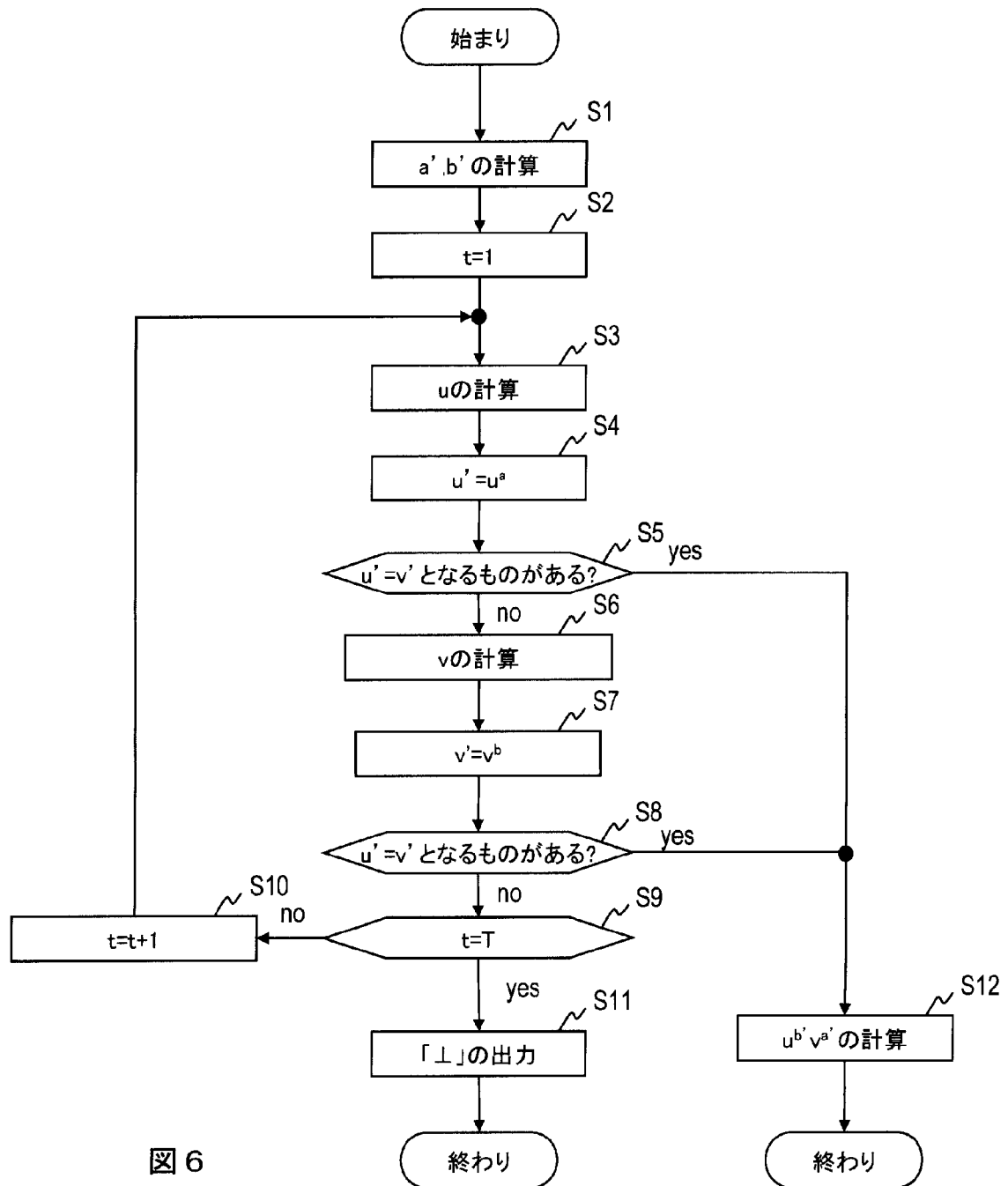


図 6

[図7]

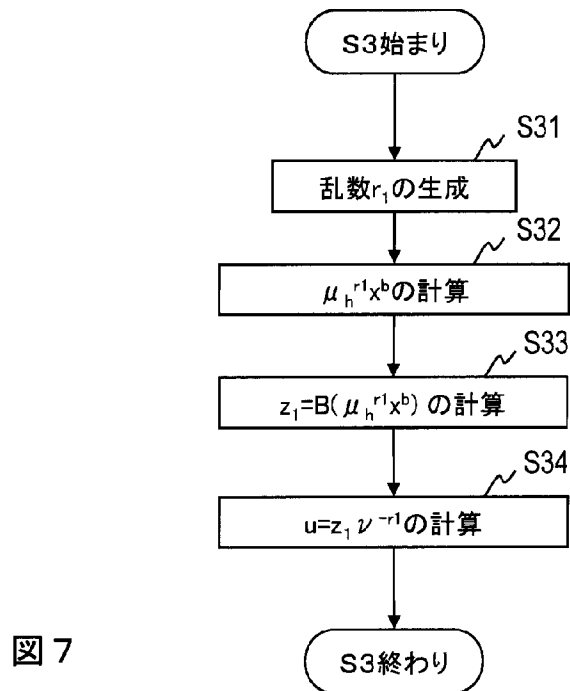


図 7

[図8]

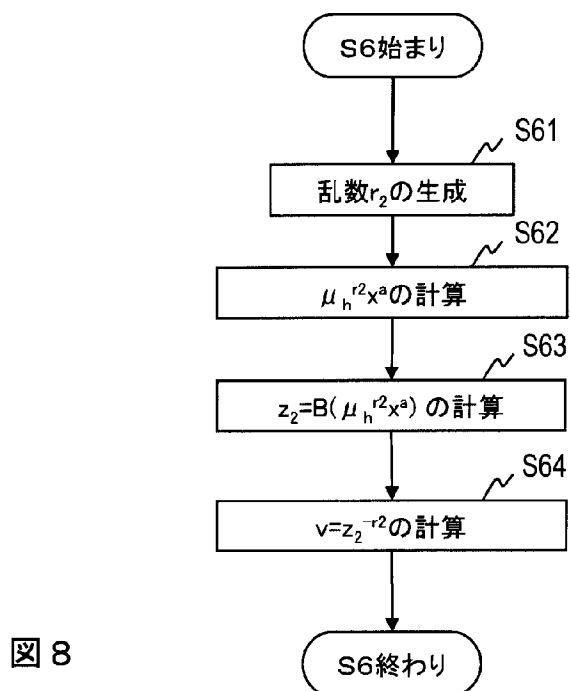


図 8

[図9]

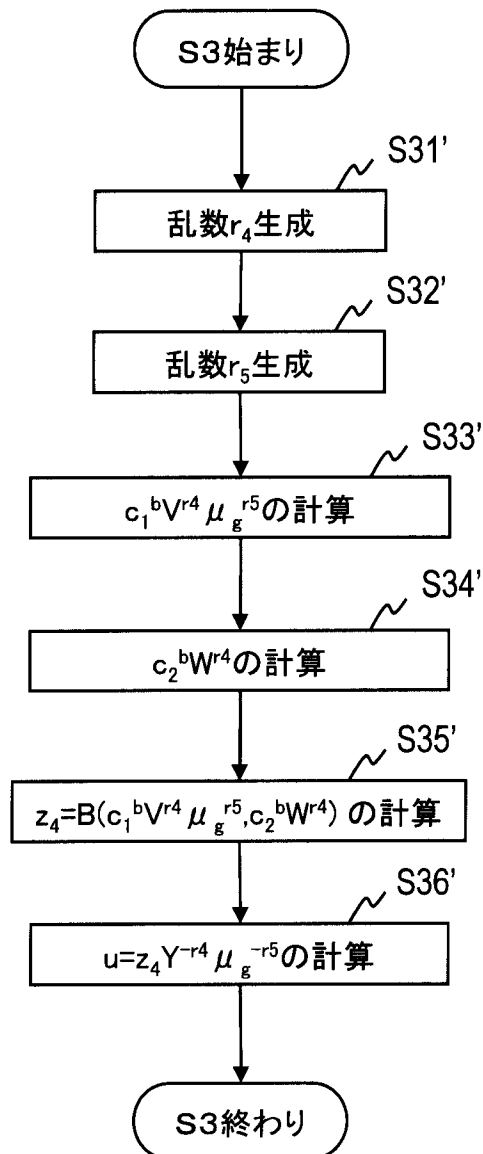


図 9

[図10]

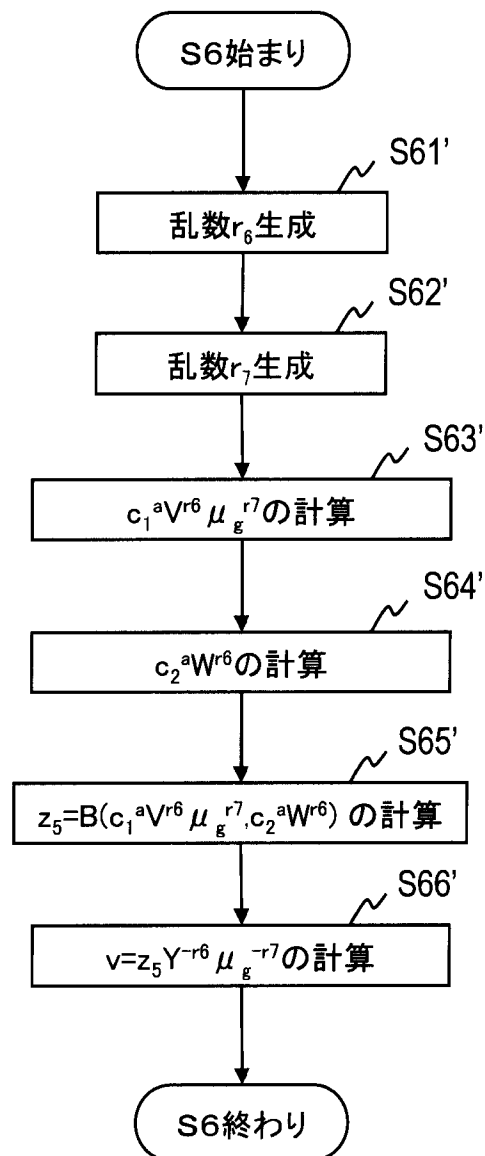


図 1 0

[図11]

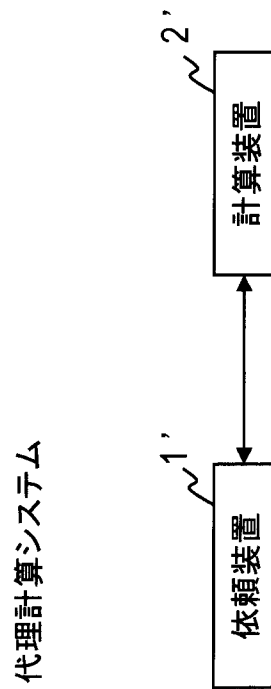


図11

[図12]

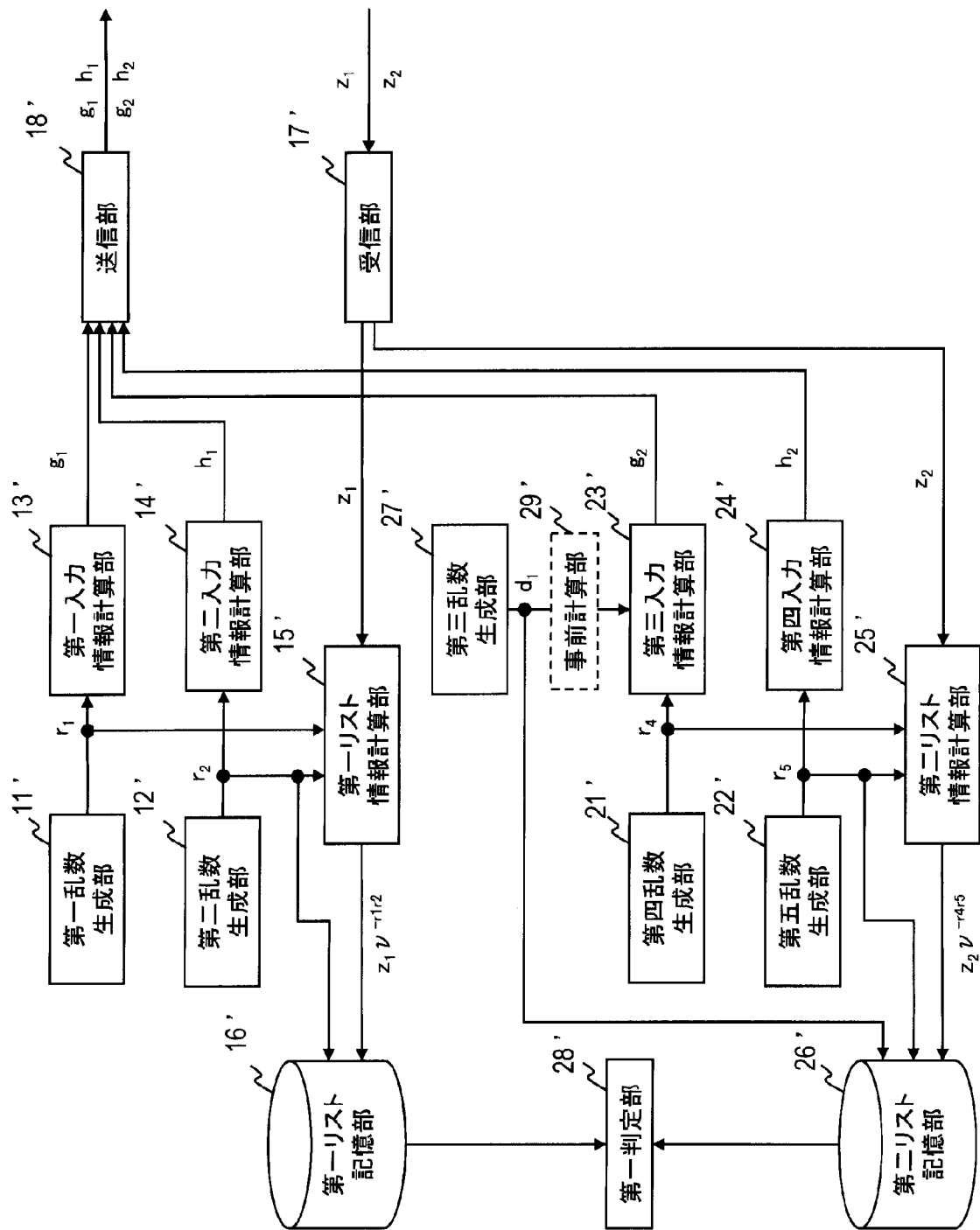


図12

[図13]

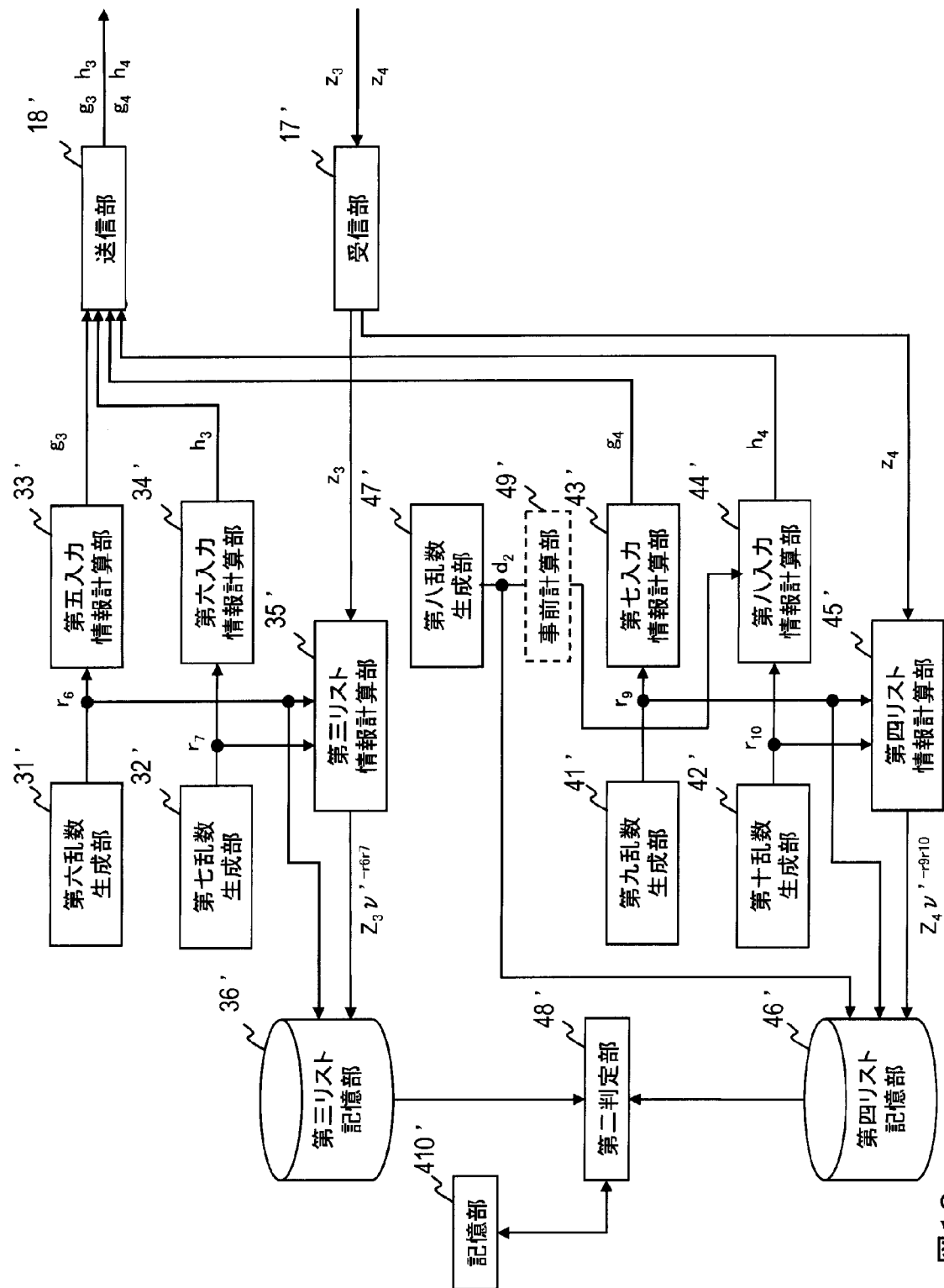


図13

[図14]

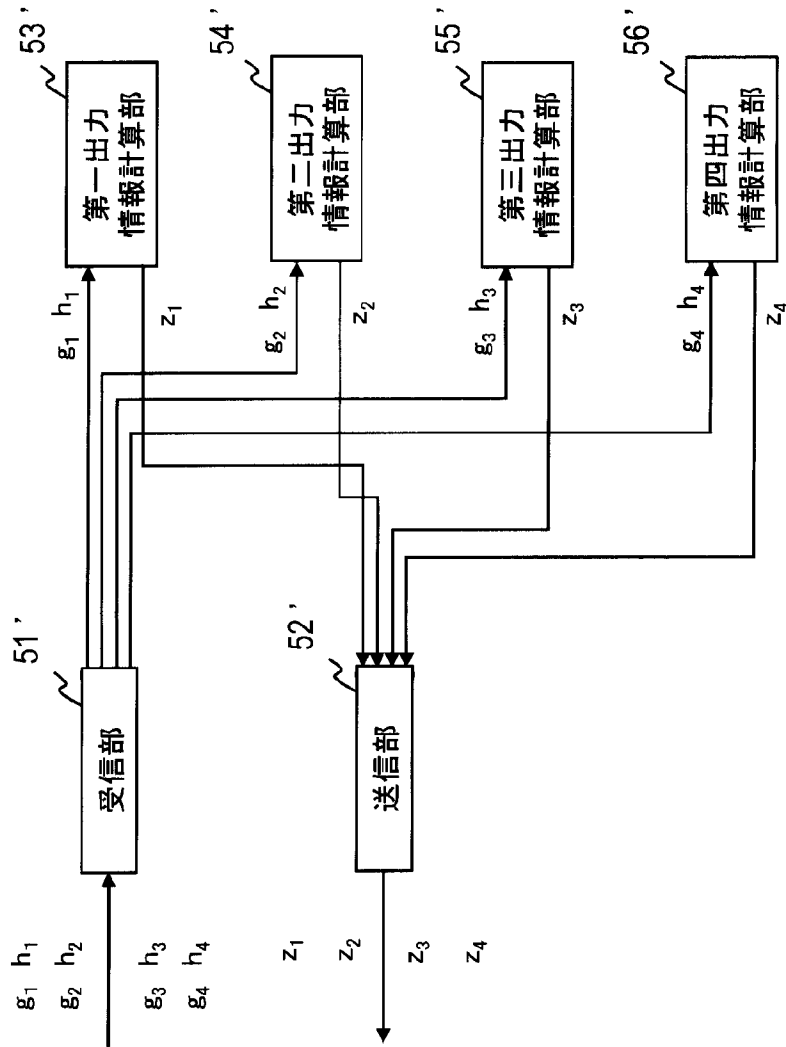


図14

[図15]

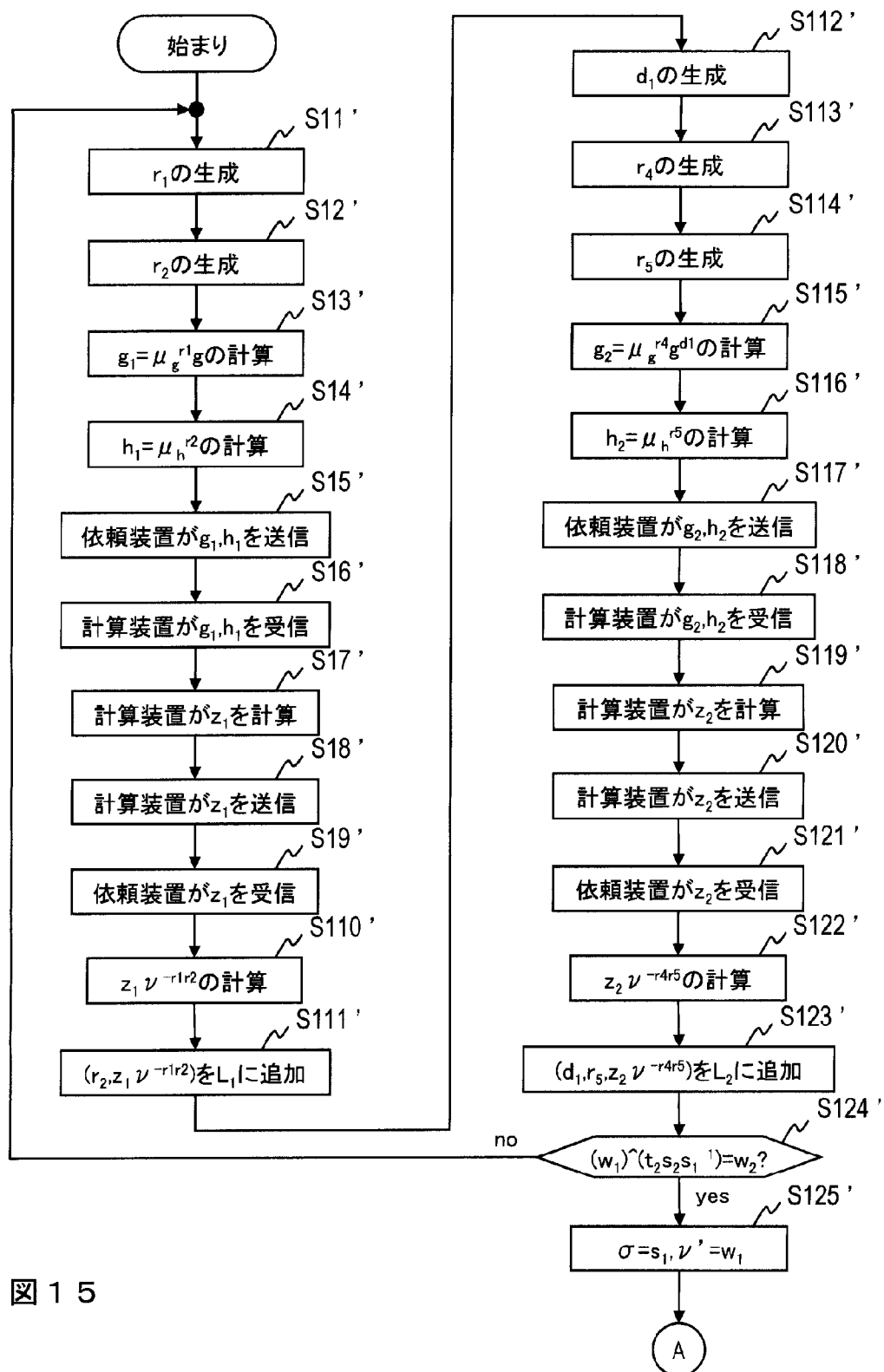


図 1 5

[図16]

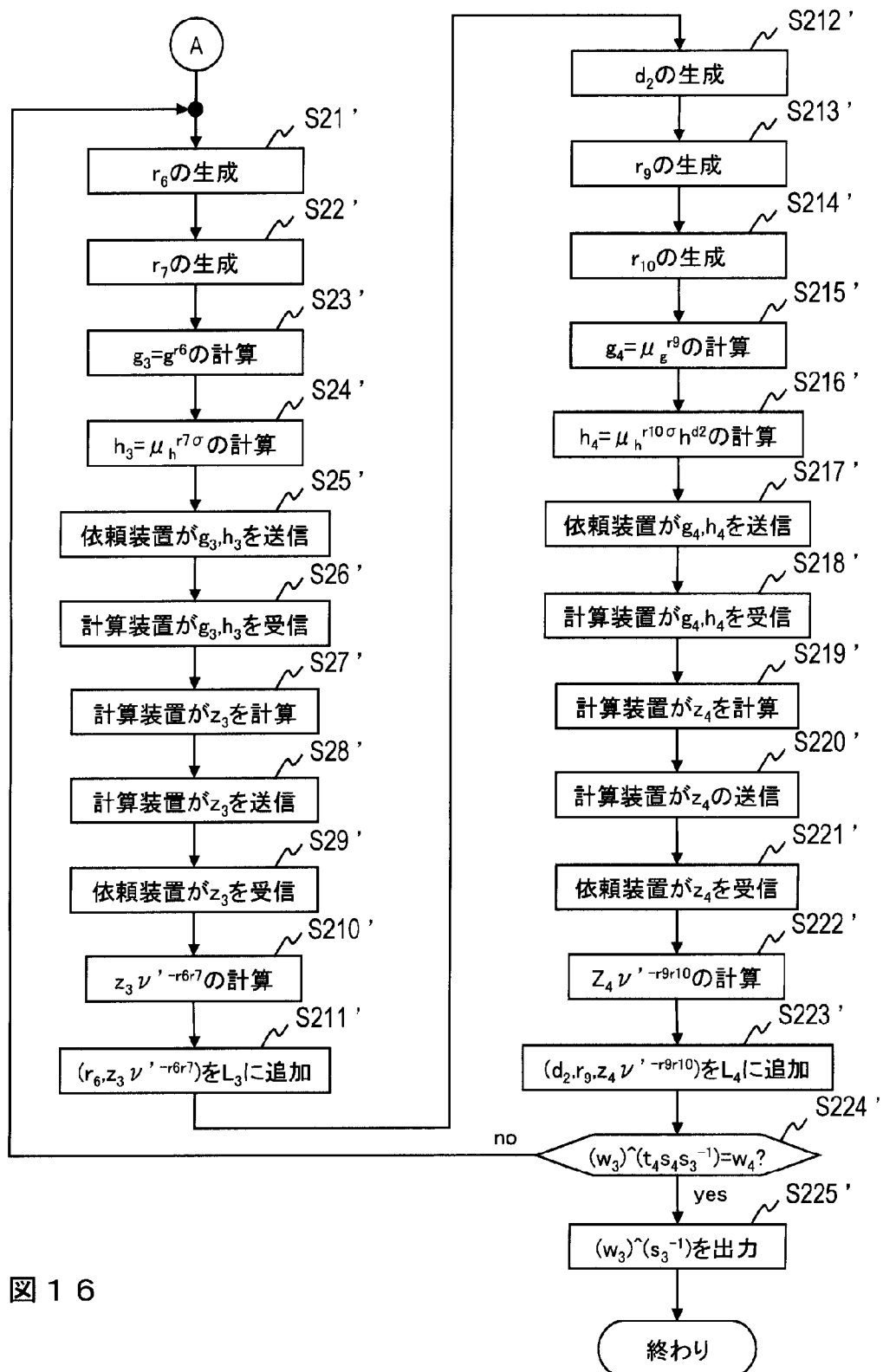


図 1 6

[図17]

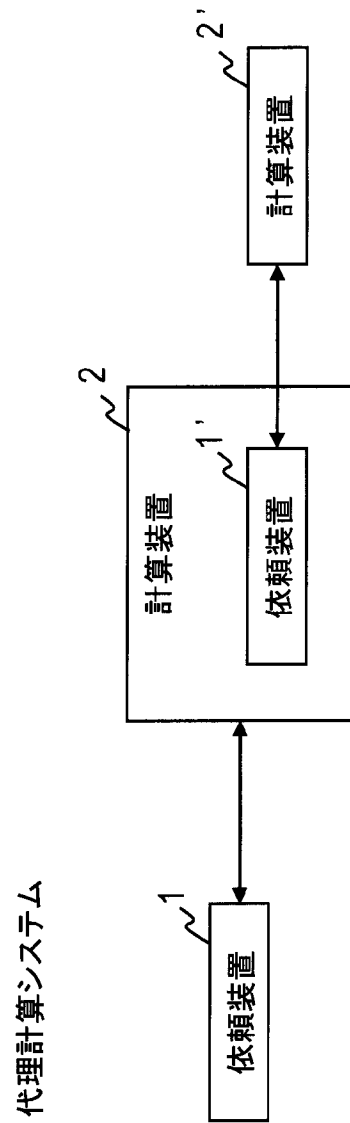


図17

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/050278

A. CLASSIFICATION OF SUBJECT MATTER

G09C1/00(2006.01) i, H04L9/20(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, H04L9/20

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	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

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	Manuel Blum and Hal Wasserman, "Reflections on the Pentium Division Bug", IEEE TRANSACTIONS ON COMPUTERS, 1996.04, Volume: 45, Issue: 4, p.385-393, [retrieved on 2011-02-04]. Retrieved from the Internet:<URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=494097>.	1-19
A	JP 2002-82609 A (Toyo Communication Equipment Co., Ltd.), 22 March 2002 (22.03.2002), entire text; all drawings (Family: none)	1-19

☒ 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
08 February, 2011 (08.02.11)

Date of mailing of the international search report
22 February, 2011 (22.02.11)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2011/050278

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Tsutomu MATSUMOTO, Hideki IMAI, "How to ask and verify oracles for speeding up secret computations", IEICE Technical Report, 19 May 1989 (19.05.1989), vol.89, no.45, pages 21 to 28	1-19
A	Tsutomu MATSUMOTO, Hideki IMAI, "How to ask and verify oracles for speeding up secret computations. Part 2", IEICE Technical Report, 21 July 1989 (21.07.1989), vol.89, no.145, pages 13 to 20	1-19
A	Tsutomu MATSUMOTO, Hideki IMAI, "How to ask and verify oracles for speeding up secret computations. Part 3", IEICE Technical Report, 25 September 1989 (25.09.1989), vol.89, no.215, pages 25 to 28	1-19
P,A	Tsuyoshi YAMAMOTO, Tetsutaro KOBAYASHI, "Jun Dogata Shazo ni Taisuru Jiko Teisei ni Tsuite", 2010 Nen Symposium on Cryptography and Information Security Gaiyoshu, 19 January 2010 (19.01.2010), 2D2 Suron Oyo, 2D2-3	1-19

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G09C1/00(2006.01)i, H04L9/20(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. G09C1/00, H04L9/20

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 1 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 1 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 1 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	Manuel Blum and Hal Wasserman, "Reflections on the Pentium Division Bug", IEEE TRANSACTIONS ON COMPUTERS, 1996.04, Volume: 45, Issue: 4, p.385-393, [retrieved on 2011-02-04]. Retrieved from the Internet:<URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=494097>.	1 - 1 9
A	JP 2002-82609 A (東洋通信機株式会社) 2002.03.22, 全文, 全図 (ファミリーなし)	1 - 1 9

☒ 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

0 8 . 0 2 . 2 0 1 1

国際調査報告の発送日

2 2 . 0 2 . 2 0 1 1

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）

青木 重徳

5 S

4 2 2 9

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

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	松本勉, 今井秀樹, “検算可能な依頼計算”, 電子情報通信学会技術研究報告, 1989.05.19, V o l . 8 9, N o . 4 5, p . 2 1 – 2 8	1 – 1 9
A	松本勉, 今井秀樹, “検算可能な依頼計算 (その2)”, 電子情報通信学会技術研究報告, 1989.07.21, V o l . 8 9, N o . 1 4 5, p . 1 3 – 2 0	1 – 1 9
A	松本勉, 今井秀樹, “検算可能な依頼計算 (その3)”, 電子情報通信学会技術研究報告, 1989.09.25, V o l . 8 9, N o . 2 1 5, p . 2 5 – 2 8	1 – 1 9
P, A	山本剛, 小林鉄太郎, “準同型写像に対する自己訂正について”, 2010年暗号と情報セキュリティシンポジウム概要集, 2010.01.19, 2 D 2 数論応用, 2 D 2 – 3	1 – 1 9