

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2009年7月30日 (30.07.2009)

PCT

(10) 国際公開番号
WO 2009/093603 A1(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2009/050857

(22) 国際出願日: 2009年1月21日 (21.01.2009)

(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2008-010928 2008年1月21日 (21.01.2008) JP
特願2008-010929 2008年1月21日 (21.01.2008) 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): 千田 浩司

(CHIDA, Koji) [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, 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, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

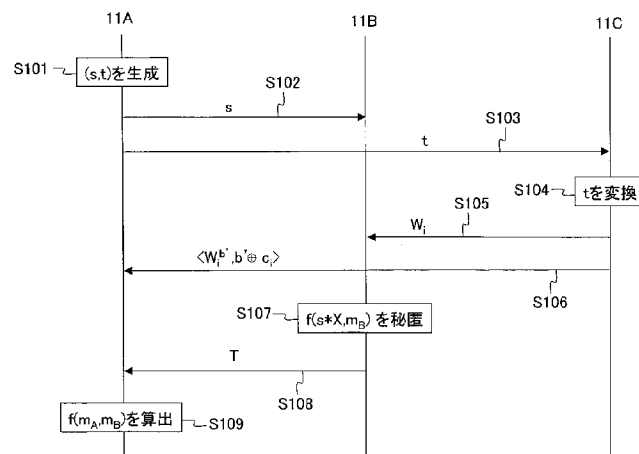
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY,

/ 続葉有 /

(54) Title: SECURE COMPUTING SYSTEM

(54) 発明の名称: 秘密計算システム

[図5]



S101 GENERATE (s, t)

S104 CONVERT t

S107 CONCEAL $f(s * X, m_B)$ S109 COMPUTE $f(m_A, m_B)$

(57) Abstract: A third secure computing device generates data W_b corresponding to the bits b of a fragment t satisfying $m_A = s * t$ with respect to a first input value m_A and an operator $*$ and data $W(1-b)$ corresponding to the inverted bits $(1-b)$ of the bits b , transmits the data W_b to a first secure computing device, and transmits the data W_b and data W including data $W(1-b)$ to a second secure computing device. The second secure computing device creates data T which includes a concealed logical circuit function $f(s * X)$ defined by embedding a fragment s in a logical circuit function f and which enables production of a computation result $f(m_A)$ from the data T itself and the data W_b . The created data T is transmitted to the first secure computing device. The first secure computing device computes the computation result $f(m_A)$ from the data T and data W_b .

/ 続葉有 /

WO 2009/093603 A1



KG, KZ, MD, RU, TJ, TM), ヨーロッパ (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

(57) 要約: 第3の秘密計算装置は、第1の入力値 mA 及び演算子 $*$ に対して $mA = s * t$ を満たす断片 t の各ビット b に対応した各データ Wb と、各ビット b の各反転ビット $(1-b)$ に対応した各データ $W(1-b)$ とを生成し、データ Wb を第1の秘密計算装置に送信し、データ Wb 及びデータ $W(1-b)$ を含むデータ W を第2の秘密計算装置に送信する。第2の秘密計算装置は、 $mA = s * t$ を満たす断片 s と論理回路関数 f とデータ W とを用い、論理回路関数 f に断片 s が埋め込まれた論理回路関数 $f(s * X)$ が秘匿されたデータ T であって、当該データ T とデータ Wb とから演算結果 $f(mA)$ を求めることができるものを生成し、データ T を第1の秘密計算装置に送信する。第1の秘密計算装置は、データ T とデータ Wb とを用いて演算結果 $f(mA)$ を算出する。

明 細 書

秘密計算システム

技術分野

[0001] 本発明は暗号応用技術に関し、特に、入力値を秘匿したまま、その入力値に対する演算の結果を得る技術に関する。

背景技術

[0002] 非特許文献1には、入力値を秘匿したままで演算結果を得る技術が開示されている。図1は、非特許文献1に開示された技術を用いた秘密計算システムの構成を示すブロック図である。図1を参照すると、秘密計算システムは、秘密計算装置81Aと秘密計算装置81Bを有している。

[0003] 秘密計算装置81Aは、論理回路関数 $f(x, y)$ と、 x への入力となるビット列 m_A とを保有している。秘密計算装置81Bは、同じく論理回路関数 $f(x, y)$ と、 y への入力となるビット列 m_B とを保有している。

[0004] 秘密計算装置81Aと秘密計算装置81Bが互いに通信することにより、秘密計算装置81Aが m_B を容易に復元できるデータを得ることなく、秘密計算装置81Bが m_A を容易に復元できるデータを得ることなく、秘密計算装置81A, Bのいずれか一方または両方が論理回路関数 $f(x, y)$ の演算結果 $f(m_A, m_B)$ を得る。

[0005] なお、論理回路関数 $f(x, y)$ は、1又は複数の論理ゲート g の組み合わせで実現できる。論理ゲート g は、入力された1つ又は2つのビットに対して所定の論理演算を行い、その結果を示す1つのビットを出力する。論理ゲートの例は、ANDゲート、ORゲートなどである。また、各論理ゲート g の入出力系列をワイヤーと呼び、入力側のワイヤーを入力ワイヤーと呼び、出力側のワイヤーを出力ワイヤーと呼ぶ。

[0006] 非特許文献1に開示された方法について概説する。以下に、一例として、秘密計算装置81Aが $f(m_A, m_B)$ を得るための処理手順を挙げる。

[0007] [ステップC1-1]

論理回路関数 $f(x, y)$ と、 y への入力となるビット列 m_B とを保有する秘密計算装置Bは、論理回路関数 $f(x, y)$ を構成する各論理ゲートの真理値表を秘匿することで論

理回路関数 $f(x, y)$ を秘匿する。

[0008] 論理ゲートの真理値表は以下になる。なお、ANDゲートの例では、 $g(0, 0) = g(0, 1) = g(1, 0) = 0$, $g(1, 1) = 1$ である。

入力ワイヤー	出力ワイヤー
0, 0	$g(0, 0)$
0, 1	$g(0, 1)$
1, 0	$g(1, 0)$
1, 1	$g(1, 1)$

[0009] 論理ゲートを秘匿する場合、秘密計算装置Bは、各入力ワイヤーと出力ワイヤーとに、それぞれ、各ワイヤーの値に対応する固定長の乱数と、各ワイヤーの値に対応するランダムビットとの組を対応付ける。そして、対応付けられた(固定長の乱数, ランダムビット)を用いて真理値表を再構成することで真理値表を秘匿する。ただし、これだけでは、各ワイヤーの値と(固定長の乱数, ランダムビット)との対応を知らない者であっても、出力ワイヤーに対応する(固定長の乱数, ランダムビット)の組み合わせから、論理ゲートの内容が推測できてしまう。そのため、擬似ランダム関数を用い、更なる秘匿を行う。これにより、論理ゲートを秘匿できる。そして、論理回路関数 $f(x, m_B)$ を構成する各論理ゲートについて同様な秘匿化を実行することで、論理回路関数 $f(x, m_B)$ を秘匿できる。

[0010] 具体的には、秘密計算装置Bは、以下の(a)～(d)を実行することにより、論理回路関数 $f(x, m_B)$ を秘匿する。

(a) 秘密計算装置81Bは、論理回路関数 $f(x, m_B)$ の各ワイヤー i に対して、固定長の乱数

[0011] [数1]

$$w_i^0, w_i^1$$

を生成し、それぞれ0, 1に対応させる。

(b) 次に、秘密計算装置81Bはランダムビット $c_i \in \{0, 1\}$ を生成する。 c_i はランダム化されたラベルとして用いる。

(c) 更に、秘密計算装置81Bは、

[0012] [数2]

$$(\langle W_i^0, c_i \rangle, \langle W_i^1, \bar{c}_i \rangle)$$

をワイヤーiに対応させる。ここで

[0013] [数3]

$$\bar{c} = 1 - c$$

とする。なお、 $\langle \alpha, \beta \rangle$ は α が β に対応することを意味する。

(d)次に、秘密計算装置81Bは、i, jを入力ワイヤー、kを出力ワイヤーとする論理ゲートgに対して、4つのラベル付きデータ

[0014] [数4]

$$\begin{aligned} c_i, c_j &: (W_k^{g(0,0)}, g(0,0) \oplus c_k) \oplus F_{W_i^0}(c_j) \oplus F_{W_j^0}(c_i), \\ c_i, \bar{c}_j &: (W_k^{g(0,1)}, g(0,1) \oplus c_k) \oplus F_{W_i^0}(\bar{c}_j) \oplus F_{W_j^1}(c_i), \\ \bar{c}_i, c_j &: (W_k^{g(1,0)}, g(1,0) \oplus c_k) \oplus F_{W_i^1}(c_j) \oplus F_{W_j^0}(\bar{c}_i), \\ \bar{c}_i, \bar{c}_j &: (W_k^{g(1,1)}, g(1,1) \oplus c_k) \oplus F_{W_i^1}(\bar{c}_j) \oplus F_{W_j^1}(\bar{c}_i), \end{aligned}$$

を生成し、それらをランダムな順番に並べたデータT_gを生成する。ここでコロンの左側をラベル、右側をデータとし、F_W(x)はx, Wを入力として、x, Wに対して一義的に定まる固定長の乱数を出力する関数(擬似ランダム関数)である。また、

[0015] [数5]

$$\alpha \oplus \beta$$

は α と β との排他的論理和を示す。また、

[0016] [数6]

$$(\alpha, \beta) \oplus \gamma$$

は、 α と β とのビット連結値 $\alpha \parallel \beta$ と γ との排他的論理和を意味する。

[0017] また、論理回路関数fの最終段のゲートgに対応するT_gのc_kは0に設定しておく。

上記のようなT_gは、論理回路関数f(x, m_B)を構成する各ゲートについて生成され、生成されたT_gの集合Tは、論理回路関数f(x, m_B)の秘匿化データとして秘密計算装置81Aに送信される。

[0018] [ステップC1-2]

xへの入力となるビット列m_Aを保有する秘密計算装置81Aは、秘密計算装置81B

と1-out-of-2 Oblivious Transferプロトコルを実行する。これにより、秘密計算装置81Aは、 m_A のビット $b \in \{0, 1\}$ を入力とするワイヤーに対応するデータ

[0019] [数7]

$$\langle w_i^b, b \oplus c_i \rangle$$

を得る。

[0020] [ステップC1-3]

続いて、秘密計算装置81Aは、秘密計算装置81Bから受信したデータ T_g と、

[0021] [数8]

$$\langle w_i^b, b \oplus c_i \rangle$$

とを用いて、論理回路関数 f の最終段の論理ゲート g のワイヤーの出力

[0022] [数9]

$$\langle w_k^{\hat{b}}, \hat{b} \oplus c_k \rangle$$

を算出する。

[0023] [ステップC1-4]

更に、秘密計算装置81Aは、

[0024] [数10]

$$\langle w_k^{\hat{b}}, \hat{b} \oplus c_k \rangle$$

から、演算結果 $f(m_A, m_B)$ のビット

[0025] [数11]

$$\hat{b}$$

を得る。

[0026] [ステップC1-3の詳細]

上記処理手順におけるステップC1-3では、秘密計算装置81Aは、入力ワイヤー i , j 、出力ワイヤー k のゲートに対応するデータ T_g と、

[0027] [数12]

$$\langle w_i^b, b \oplus c_i \rangle, \langle w_j^d, d \oplus c_j \rangle \quad (d \in \{0, 1\}) \quad (1)$$

とが与えられたとき、先ずデータ T_g からラベル

[0028] [数13]

$$(b \oplus c_i, d \oplus c_j)$$

に対応するデータ

[0029] [数14]

$$(W_k^{g(b,d)}, g(b,d) \oplus c_k) \oplus F_{w_i^h}(d \oplus c_j) \oplus F_{w_j^g}(b \oplus c_i) \quad (2)$$

を取り出す。また、秘密計算装置81Aは、

[0030] [数15]

$$F_{w_i^h}(d \oplus c_j) \oplus F_{w_j^g}(b \oplus c_i) \quad (3)$$

を計算する。秘密計算装置81Aは、式(2)と式(3)との排他的論理和を行い、出力ワイヤーに対応するデータ

[0031] [数16]

$$(W_k^{g(b,d)}, g(b,d) \oplus c_k) \quad (4)$$

を得る。そして、秘密計算装置81Aは、例えば、出力ワイヤーに対応するデータを他の論理ゲートの入力ワイヤーの1つのデータとし、他の論理ゲートについても同様の処理を行い、最終的にfの最終段の論理ゲートgのワイヤーの出力を得る。

[0032] [ステップC1-4の詳細]

論理回路関数fの最終段のゲートgに対応する $T_{g,k}$ の c_k を0に設定しておくことで、

[0033] [数17]

$$\langle W_k^{\hat{b}}, \hat{b} \oplus c_k \rangle = \langle W_k^{\hat{b}}, \hat{b} \oplus 0 \rangle = \langle W_k^{\hat{b}}, \hat{b} \rangle$$

となるため、秘密計算装置81Aは、ステップC1-4において、

[0034] [数18]

$$\hat{b}$$

を得ることができる。

[0035] 以上説明したように、非特許文献1の方法では、第2のステップにおいて秘密計算装置81Aと秘密計算装置81Bが1-out-of-2 Oblivious Transferプロトコルを実行する必要がある。1-out-of-2 Oblivious Transferプロトコルは、秘密計算装置81Bがデータ d_0, d_1 を保有し、秘密計算装置81Aがビットbを保有するとき、

秘密計算装置81Aは d_b を得ることができるが、

[0036] [数19]

$$d_g$$

を得ることはできず、かつ秘密計算装置81Bは b を得ることができないような特徴をもつプロトコルである。このプロトコルを用いることで、秘密計算装置81Aから秘密計算装置81Bへ、 m_A のビット b が漏洩することを防止できるとともに、 T_g に秘匿化されている論理回路関数 $f(x, m_B)$ の情報が秘密計算装置81Aに漏洩することを防止できる。なお、このプロトコルの詳細は、非特許文献2に説明がある。

[0037] 非特許文献3には、入力値を秘匿したままで演算結果を得る他の技術が開示されている。図2は、非特許文献3に開示された技術を用いた秘密計算システムの構成を示すブロック図である。図2を参照すると、秘密計算システムは、複数の変換装置 $90_1 \sim 90_N$ と秘密計算装置91A, 91Bとを有している。2つの秘密計算装置91A, 91Bによって秘密計算装置群91をなしている。

[0038] 秘密計算装置91A, 91Bからなる秘密計算装置群91は、各変換装置 $90_1 \sim 90_N$ が保有するデータ m_n ($1 \leq n \leq N$)を用いて、入力値 m_n を容易に復元できるデータを得ることなく、論理回路関数 $f(x_1, \dots, x_N)$ の演算結果 $f(m_1, \dots, m_N)$ を求める。

[0039] 以下にその処理手順について概説する。

[ステップC2-1]

まず、秘密計算装置91Bは、以下の(a)～(d)を実行することにより、論理回路関数 f を秘匿する。そして、秘密計算装置91Bは、論理回路関数 f に対応するデータ T_g を、論理回路関数 $f(x_1, \dots, x_N)$ の秘匿化データとして秘密計算装置91Aに送信する。

(a) 秘密計算装置91Bは論理回路関数 $f(x_1, \dots, x_N)$ の各ワイヤー i に対して、固定長の乱数

[0040] [数20]

$$w_i^0, w_i^1$$

を生成し、それぞれ0, 1に対応させる。

(b) 次に、秘密計算装置91Bは、ランダムビット $c_i \in \{0, 1\}$ を生成する。

(c) 更に、秘密計算装置91Bは、

[0041] [数21]

$$\langle W_i^0, c_i \rangle, \langle W_i^1, \bar{c}_i \rangle$$

をワイヤーiに対応させる。ここで

[0042] [数22]

$$\bar{c} = 1 - c$$

とする。

(d) 更に、秘密計算装置91Bは、i, jを入力ワイヤー、kを出力ワイヤーとする論理ゲートgに対して、4つのラベル付きデータ

[0043] [数23]

$$\begin{aligned} c_i, c_j &: (W_k^{g(0,0)}, g(0,0) \oplus c_k) \oplus F_{W_i^0}(c_j) \oplus F_{W_j^0}(c_i), \\ c_i, \bar{c}_j &: (W_k^{g(0,1)}, g(0,1) \oplus c_k) \oplus F_{W_i^0}(\bar{c}_j) \oplus F_{W_j^1}(c_i), \\ \bar{c}_i, c_j &: (W_k^{g(1,0)}, g(1,0) \oplus c_k) \oplus F_{W_i^1}(c_j) \oplus F_{W_j^0}(\bar{c}_i), \\ \bar{c}_i, \bar{c}_j &: (W_k^{g(1,1)}, g(1,1) \oplus c_k) \oplus F_{W_i^1}(\bar{c}_j) \oplus F_{W_j^1}(\bar{c}_i), \end{aligned}$$

[0044] を生成し、それらをランダムな順番に並べたデータ T_g を生成する。データ T_g の集合 T_g が、論理回路関数 $f(x_1, \dots, x_N)$ の秘匿化データとして秘密計算装置91Aに送信される。

[0045] [ステップC2-2]

各変換装置 $90_1 \sim 90_N$ が、秘密計算装置91A、91Bとともに、proxy 1-out-of-2 Oblivious Transferプロトコルを実行することにより、秘密計算装置91Aはmの各ビットbの入力ワイヤーiに対応するデータ

[0046] [数24]

$$\langle W_i^b, b \oplus c_i \rangle$$

を得る。

[0047] [ステップC2-3]

更に、秘密計算装置91Aは、データ T_g と、

[0048] [数25]

$$\langle W_i^b, b \oplus c_i \rangle$$

とを用いて、論理回路関数 f の最終段の論理ゲート g のワイヤーの出力

[0049] [数26]

$$\langle w_k^{\hat{b}}, \hat{b} \oplus c_k \rangle$$

を得る。

[0050] (ステップC2-4)

更に、秘密計算装置91Aは、

[0051] [数27]

$$\langle w_k^{\hat{b}}, \hat{b} \oplus c_k \rangle$$

から、演算結果 $f(m_1, \dots, m_N)$ のビット

[0052] [数28]

$$\hat{b}$$

を得る。

[0053] 上記処理手順のステップC2-2では、proxy 1-out-of-2 Oblivious Transferプロトコルが用いられている。このプロトコルは、1-out-of-2 Oblivious Transferプロトコルを拡張したプロトコルである。このプロトコルによれば、変換装置90₁～90_Nが保有しているデータに関する情報であるビット b を秘密計算装置91Aに知られることなく、変換装置90₁～90_Nの代わりに秘密計算装置91Aが

[0054] [数29]

$$\langle w_i^b, b \oplus c_i \rangle$$

を算出することができる。

非特許文献1:A. C. Yao, How to generate and exchange secrets, Proc. of FOCS '86, pp. 162-167, IEEE Press, 1986.

非特許文献2:S. Even, O. Goldreich and A. Lempel, A randomized protocol for signing contracts, Communications of the ACM, Vol. 28, No. 6, pp. 637-647, 1985.

非特許文献3:M. Naor, B. Pinkas, and R. Sumner, Privacy preserving auctions and mechanism design, Proc. of ACM EC '99, pp. 129-139, ACM Press, 1999.

発明の開示

発明が解決しようとする課題

- [0055] 上述したように、非特許文献1に開示された方法では、秘密計算装置81A, 81Bが1-out-of-2 Oblivious Transferプロトコルを実行する必要がある。また、特許文献3に開示された方法では、変換装置 $90_1 \sim 90_N$ 及び秘密計算装置91A, 91Bが、proxy 1-out-of-2 Oblivious Transferプロトコルを実行する必要がある。
- [0056] D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella, Fairplay — a secure two-party computation system, Proc. of USENIX Security Symposium, pp. 287–302, USENIX, 2004. という文献によれば、実装上、1-out-of-2 Oblivious Transferプロトコルを実行するための計算量が秘密計算システム全体の計算量の大部分を占めると報告されている。
- [0057] また、1-out-of-2 Oblivious Transferプロトコルを拡張したproxy 1-out-of-2 Oblivious Transferプロトコルを実行する際に必要となる計算量は、1-out-of-2 Oblivious Transferプロトコルと同程度である。
- [0058] したがって、実装上、これらのプロトコルに関連する処理量を削減することができれば、秘密計算システムの負荷を低減することができる。

課題を解決するための手段

- [0059] 本発明の第1態様は、第1の秘密計算装置と、論理回路関数 f を格納した第2の秘密計算装置と、第3の秘密計算装置とによって実行される。
- [0060] 第3の秘密計算装置は、第1の入力値 m_A 及び演算子 $*$ に対して $m_A = s * t$ を満たす断片 t の各ビット b に対応した各データ W_b と、各ビット b の各反転ビット $(1-b)$ に対応した各データ $W(1-b)$ とを生成する。第3の秘密計算装置は、データ W_b を第1の秘密計算装置に送信し、ビット b 及び反転ビット $(1-b)$ とデータ W_b 及びデータ $W(1-b)$ との対応を特定せずに、データ W_b 及びデータ $W(1-b)$ を含むデータ W を第2の秘密計算装置に送信する。
- [0061] 第2の秘密計算装置は、 $m_A = s * t$ を満たす断片 s と論理回路関数 f とデータ W とを用い、論理回路関数 f に断片 s が埋め込まれた論理回路関数 $f(s * X)$ が秘匿されたデ

ータTであって、当該データTとデータWbとから演算結果 $f(mA)$ を求めることができるものを生成する。第2の秘密計算装置は、データTを第1の秘密計算装置に送信する。

[0062] 第1の秘密計算装置には、データTとデータWbとが入力され、データTとデータWbとを用いて演算結果 $f(mA)$ を算出する。

本発明の第2態様は、論理回路関数 $f(x)$ を格納した第1の秘密計算装置と、第2の秘密計算装置とによって実行される。

[0063] 第1の秘密計算装置には、入力値 m から分割された断片Aと断片Bとのうち断片Bが入力される。第1の秘密計算装置は、論理回路関数 $f(x)$ と断片Bとを用い、論理回路関数 $f(x)$ が秘匿されたデータTであって、当該データTと断片Aとから演算結果 $f(m)$ を求めることのできるものを生成する。

第2の秘密計算装置には、断片AとデータTとが入力され、断片AとデータTとを用いて演算結果 $f(m)$ を算出する。

発明の効果

[0064] 本発明によれば、論理回路関数 f の入力値の情報が2つの断片に分割され、分割された2つの断片がそれぞれ異なる秘密計算装置に入力されて処理される。その結果、1-out-of-2 Oblivious Transferプロトコルやproxy 1-out-of-2 Oblivious Transferプロトコルに関する処理負荷を軽減でき、秘密計算装置の負荷を大幅に低減できる。

図面の簡単な説明

[0065] [図1]図1は、非特許文献1に開示された技術を用いた秘密計算システムの構成を示すブロック図である。

[図2]図2は、非特許文献3に開示された技術を用いた秘密計算システムの構成を示すブロック図である。

[図3]図3は、第1の実施形態の秘密計算システムの構成を示すブロック図である。

[図4]図4(A)(B)(C)は、第1の実施形態の秘密計算システムが含む秘密計算装置11Aの構成を示すブロック図である。

[図5]図5は、第1の実施形態の秘密計算システムの動作の具体例を示すシーケンス

図である。

[図6]第2の実施形態の秘密計算システムの構成を示すブロック図である。

[図7]図7(A)(B)(C)は、第2の実施形態の秘密計算システムが含む秘密計算装置の構成を示すブロック図である。

[図8]図8は、秘密計算システムが含む変換装置の構成を示すブロック図である。

[図9]図9は、第2の実施形態の秘密計算システムの動作の具体例を示すシーケンス図である。

[図10]図10は、第3の実施形態の秘密計算システムの構成を示すブロック図である。

[図11]図11(A)(B)は、第3の実施形態の秘密計算システムが含む秘密計算装置の構成を示すブロック図である。

[図12]図12は、第3の実施形態の秘密計算システムの動作の具体例を示すシーケンス図である。

[図13]図13は、第4の実施形態の秘密計算システムの構成を示すブロック図である。

[図14]図14(A)(B)は、秘密計算システムが含む秘密計算装置の構成を示すブロック図である。

[図15]図15は、秘密計算システムが含む変換装置の構成を示すブロック図である。

[図16]図16は、第4の実施形態の秘密計算システムの動作の具体例を示すシーケンス図である。

符号の説明

[0066] 1～4 秘密計算システム

発明を実施するための最良の形態

[0067] 本発明の実施形態を、図面を参照して詳細に説明する。

〔第1の実施形態〕

本実施形態の秘密計算システムは3つの秘密計算装置からなる。この秘密計算システムを構成する2つの秘密計算装置は、それぞれ、互いに独立な入力値を保持している。本実施形態の秘密計算システムは、秘密計算装置によって保有された入力値が他の秘密計算装置に知られることなく、当該入力値に対する論理回路関数 f の演算結果を算出する。

[0068] <構成>

図3は、第1の実施形態の秘密計算システム1の構成を示すブロック図である。また、図4(A)(B)(C)は、秘密計算システム1が含む秘密計算装置11A, 11B, 11Cの構成を示すブロック図である。

図3に示すように、秘密計算システム1は、秘密計算装置11A, 11B, 11C(第1、2、3の秘密計算装置)を有する。

[0069] 図4(A)に示すように、秘密計算装置11Aは、記憶部11AA、入力部11AB、出力部11AC、分割部11AD、ビット秘匿部11AE及び秘密計算部11AFを有する。また、図4(B)に示すように、秘密計算装置11Bは、記憶部11BA、入力部11BB、出力部11BC、ビット秘匿部11BD、及び関数秘匿部11BFを有する。また、図4(C)に示すように、秘密計算装置11Cは、記憶部11CA、入力部11CB、出力部11CC、ビット秘匿部11CD及び選択部11CEを有する。

[0070] なお、秘密計算装置11A, 11B, 11Cの例は、CPU(central processing unit)、RAM(random-access memory)、ROM(read-only memory)、通信装置、入力インタフェース、出力インタフェースなどからなる公知のコンピュータに所定のプログラムが読み込まれて構成された装置である。また、秘密計算装置11A, 11B, 11Cが集積回路を含んでもよい。

[0071] <処理>

本実施形態の処理は、前述した本発明の第1態様の一例である。本実施形態では、前処理によって、秘密計算装置11Aの記憶部11AAに入力値 m_A が格納され、秘密計算装置11Bの記憶部11BAに入力値 m_B と論理回路関数 $f(x, y)$ とが格納されている。本実施形態の秘密計算システム1は、秘密計算装置11Aによって保有された入力値 m_A が秘密計算装置に知られることなく、かつ、秘密計算装置11Bによって保有された入力値 m_B が秘密計算装置に知られることなく、論理回路関数 $f(x, y)$ の演算結果 $f(m_A, m_B)$ を算出する。

[0072] まず、秘密計算装置11Aは、入力値 m_A を、演算子*に対して $m_A = s * t$ を満たす断片sと断片tの2つに分割し、断片sを秘密計算装置11Bに送信し、断片tを秘密計算装置11Cに送信する(ステップE1-1)。

[0073] 秘密計算装置11Cは、入力された断片 t の各ビット b に対応した各データ W_b と、各ビット b の各反転ビット $(1-b)$ に対応した各データ $W(1-b)$ とを生成する。そして、秘密計算装置11Cは、ビット b 及び反転ビット $(1-b)$ とデータ W_b 及びデータ $W(1-b)$ との対応を特定せずに、データ W_b 及びデータ $W(1-b)$ を含むデータ W を秘密計算装置11Bに送信し、データ W_b を秘密計算装置11Aに送信する(ステップE1-2)。

[0074] 秘密計算装置11Bは、断片 s と論理回路関数 $f(x, y)$ とデータ W と入力値 m_B を用い、論理回路関数 $f(x, y)$ に断片 s と入力値 m_B とが埋め込まれた論理回路関数 $f(s * X, m_B)$ が秘匿されたデータ T であって、当該データ T とデータ W_b とから入力値 m_A 及び入力値 m_B に対する論理回路関数 $f(x, y)$ の演算結果 $f(m_A, m_B)$ を求めることができるものを生成する。秘密計算装置11Bは、データ T を秘密計算装置11Aに送信する(ステップE1-3)。

[0075] 秘密計算装置11Aには、データ T とデータ W_b とが入力される。秘密計算装置11Aは、データ T とデータ W_b とを用いて演算結果 $f(m_A, m_B)$ を算出する(ステップE1-4, 5)。

[0076] 以下に、本実施形態の秘密計算システム1の動作の具体例を示す。

図5は、第1の実施形態の秘密計算システム1の動作の具体例を示すシーケンス図である。

[ステップE1-1]

この例では、演算子 $*$ としてXOR(排他的論理和演算子)を用いる。秘密計算装置11Aの分割部11ADが、記憶部11AAに格納された入力値 m_A を

[0077] [数30]

$$m_A = s \oplus t$$

となるランダムな断片 s, t に分割する(ステップS101)。そして、秘密計算装置11Aの出力部11ACが、断片 s を秘密計算装置11Bに送信し(ステップS102)、断片 t を秘密計算装置11Cにそれぞれ送信する(ステップS103)。

[0078] [ステップE1-2]

秘密計算装置11Cのビット秘匿部11CDは、論理回路関数 $f(s * X, m_B)$ の $m_B = s * X$ の X に対応する入力ワイヤー i ごとに、固定長の乱数であるデータ W_i^0 とランダムビッ

と c_i との組、及び、固定長の乱数である W_i^1 とランダムビット c_i の反転ビットとの組からなる

[0079] [数31]

$$W_i = (\langle W_i^0, c_i \rangle, \langle W_i^1, \bar{c}_i \rangle)$$

を生成する(「データW」の具体例)。

[0080] また、選択部11CEは、上記のように生成された W_i から、実際の t の各ビット b' に対応する組

[0081] [数32]

$$\langle W_i^{b'}, b' \oplus c_i \rangle$$

をそれぞれ選択する(ステップS104)。なお、 b' は、入力ワイヤー i への入力断片 t の下位 w 番目のビットである場合における、断片 t の下位 w 番目のビットを意味する。また、

[0082] [数33]

$$\langle W_i^{b'}, b' \oplus c_i \rangle$$

は「データ Wb 」の具体例である。

そして、秘密計算装置11Cの出力部11CCは、 W_i を秘密計算装置11Bに送信し(ステップS105)、

[0083] [数34]

$$\langle W_i^{b'}, b' \oplus c_i \rangle$$

を秘密計算装置11Aに送信する(ステップS106)。

[0084] [ステップE1-3]

秘密計算装置11Bが、以下の(a)～(d)を実行することにより、論理回路関数 $f(x, y)$ に断片 s と入力値 m_B とが埋め込まれた論理回路関数 $f(s * X, m_B)$ を秘匿する。なお、この例の論理回路関数 $f(x, y)$ に断片 s と入力値 m_B とが埋め込まれた論理回路関数 $f(s * X, m_B)$ は、断片 $X = t$ を入力として $m_A = s * X$ を復元する関数 $m_A = s * X$ と、論理回路関数 $f(x, y)$ に入力値 m_B が埋め込まれた論理回路関数 $f(x, m_B)$ とを含み、論理回路関数 $f(x, m_B)$ に関数 $m_A = s * X$ の出力値 m_A を入力して $f(m_A, m_B)$ を出力

する関数である。以下では、このような論理回路関数 $f(x, m_B)$ を構成する各論理ゲートを秘匿する。

(a) 秘密計算装置11Bのビット秘匿部11BDが、 $f(s*X, m_B)$ の各ワイヤー i に対して、固定長の乱数

[0085] [数35]

$$w_i^0, w_i^1$$

を生成し、それぞれ0, 1に対応させる。ただし、関数 $m_A = s*X$ を構成する論理ゲートのうち、 $X=t$ のビットが入力される入力ワイヤーに対しては、秘密計算装置11Cから受け取った

[0086] [数36]

$$w_i^0, w_i^1$$

を対応させる。

(b) 次に、秘密計算装置11Bのビット秘匿部11BDは、ランダムビット c_i を生成する。ただし、関数 $m_A = s*X$ を構成する論理ゲートのうち、 $X=t$ のビットが入力される入力ワイヤーに対しては、秘密計算装置11Cから受け取った c_i を用いるため、 $X=t$ のビットが入力される入力ワイヤーに対しては新たなランダムビット c_i を生成しない。

(c) 更に、秘密計算装置11Bのビット秘匿部11BDは、

[0087] [数37]

$$\langle w_i^0, c_i \rangle, \langle w_i^1, \bar{c}_i \rangle$$

をワイヤー i に対応させる。ただし、断片 s の下位 w 番目のビットに対応するワイヤー i には、

[0088] [数38]

$$\langle w_i^b, b \oplus c_i \rangle, \langle w_i^{\bar{b}}, \bar{b} \oplus c_i \rangle$$

を対応させる。ここで、 b は断片 s の下位 w 番目のビットである。

(d) 次に、秘密計算装置11Bの関数秘匿部11BFが、 i, j を入力ワイヤー、 k を出力ワイヤーとする各論理ゲート g に対して、4つのラベル付きデータ

[0089] [数39]

$$c_i, c_j : (W_k^{g(0,0)}, g(0,0) \oplus c_k) \oplus F_{W_i^0}(c_j) \oplus F_{W_j^0}(c_i),$$

$$c_i, \bar{c}_j : (W_k^{g(0,1)}, g(0,1) \oplus c_k) \oplus F_{W_i^0}(\bar{c}_j) \oplus F_{W_j^1}(c_i),$$

$$\bar{c}_i, c_j : (W_k^{g(1,0)}, g(1,0) \oplus c_k) \oplus F_{W_i^1}(c_j) \oplus F_{W_j^0}(\bar{c}_i),$$

$$\bar{c}_i, \bar{c}_j : (W_k^{g(1,1)}, g(1,1) \oplus c_k) \oplus F_{W_i^1}(\bar{c}_j) \oplus F_{W_j^1}(\bar{c}_i),$$

を生成し、それらをランダムな順番に並べたデータ T_g を生成する。この T_g の集合 T_g が論理回路関数 $f(s*X, m_B)$ を秘匿したデータとなる(ステップS107)。なお、論理回路関数 $f(s*X, m_B)$ の最終段のゲート g に対応する T_g の c_k は0に設定しておく。

[0090] 秘密計算装置11Bの出力部11BCは、 T_g の集合 T_g を論理回路関数 $f(s*X, m_B)$ の秘匿化データとして秘密計算装置11Aに送信する(ステップS108)。

[ステップE1-4]

秘密計算装置11Aの入力部11ABには、データ T_g の集合 T_g と

[0091] [数40]

$$\langle W_i^{b'}, b' \oplus c_i \rangle$$

が入力される。秘密計算装置11Aの秘密計算部11AFは、データ T_g と

[0092] [数41]

$$\langle W_i^{b'}, b' \oplus c_i \rangle$$

を用いて、論理回路関数 f の最終段の論理ゲート g のワイヤーの出力

[0093] [数42]

$$\langle W_i^{\hat{b}}, \hat{b} \oplus c_i \rangle$$

を得る。

[ステップE1-5]

秘密計算装置11Aの秘密計算部11AFは、

[0094] [数43]

$$\langle W_i^{\hat{b}}, \hat{b} \oplus c_i \rangle$$

から、演算結果 $f(m_A, m_B)$ のビット

[0095] [数44]

$$\hat{b}$$

を得る(ステップS109)。

[ステップE1-4の詳細]

上記処理手順のステップE1-4では、秘密計算装置11Aの秘密計算部11AFに、
入力ワイヤーi, j、出力ワイヤーkのゲートgに対応するT_gと、

[0096] [数45]

$$\langle W_i^{b'}, b' \oplus c_i \rangle, \langle W_j^d, d \oplus c_j \rangle \quad (d \in \{0, 1\}) \quad (5)$$

とが与えられたとき、秘密計算部11AFは、先ずT_gからラベル

[0097] [数46]

$$(b' \oplus c_i, d \oplus c_j)$$

をラベルに対応するデータ

[0098] [数47]

$$(W_k^{g(b', d)}, g(b', d) \oplus c_k) \oplus F_{W_i^{b'}}(d \oplus c_j) \oplus F_{W_j^d}(b' \oplus c_i) \quad (6)$$

を取り出す。また、秘密計算部11AFは、

[0099] [数48]

$$F_{W_i^{b'}}(d \oplus c_j) \oplus F_{W_j^d}(b' \oplus c_i) \quad (7)$$

を計算する。秘密計算部11AFは、式(6)と式(7)との排他的論理和を行い、出力ワイヤーに対応するデータ

[0100] [数49]

$$(W_k^{g(b', d)}, g(b', d) \oplus c_k) \quad (8)$$

を得る。そして、秘密計算部11AFは、例えば、出力ワイヤーに対応するデータを他のゲートの入力ワイヤーの1つのデータとし、他のゲートについても同様の処理を行い、最終的に論理回路関数fの最終段の論理ゲートgのワイヤーの出力を得る。

[0101] [ステップE1-5の詳細]

論理回路関数f(s*X, m_B)の最終段のゲートgに対応するT_gのc_kを0に設定しておくことで、

[0102] [数50]

$$\langle W_k^{\hat{b}}, \hat{b} \oplus c_k \rangle = \langle W_k^{\hat{b}}, \hat{b} \oplus 0 \rangle = \langle W_k^{\hat{b}}, \hat{b} \rangle$$

となるため、秘密計算装置11Aの秘密計算部11AFは、

[0103] [数51]

$$\hat{b}$$

を得ることができる。

[0104] 以上、説明したように、本実施形態によれば、非特許文献1の技術を用いた秘密計算システムでは全体の計算量の大部分を占めていた1-out-of-2 Oblivious Transferプロトコルを秘密計算装置11A, 11B, 11Cのいずれも実行する必要がないので、秘密計算装置11A, 11B, 11Cの負荷を大幅に低減することができる。

[0105] なお、本実施形態で追加された秘密計算装置11Cには入力値 m_A の断片 t が与えられるだけなので、秘密計算装置11Cによって入力値 m_A , m_B の秘匿性が損なわれることはない。

また、本実施形態では、XORを演算子*として用いる例を示したが、本発明はこれに限定されるものではない。例えば、加減算、乗算、その他どのような演算子を演算子*としてもよい。

[0106] [第2の実施形態]

第2の実施形態は第1の実施形態の変形例である。第2の実施形態の第1の実施形態との主な相違点は以下である。

- ・第1の実施形態では、3つの秘密計算装置から秘密計算システムが構成されていた。第2の実施形態では、N個(Nは正の整数)の変換装置と3つの秘密計算装置とから秘密計算システムが構成される。

- ・第1の実施形態では、2つの秘密計算装置がそれぞれ入力値を保持し、1つの秘密計算装置が入力値を2つの断片に分割していた。第2の実施形態では、各変換装置がそれぞれ互いに独立な入力値を保持し、各変換装置が入力値を2つの断片に分割する。

[0107] <構成>

図6は、第2の実施形態の秘密計算システム2の構成を示すブロック図である。また、図7(A)(B)(C)は、秘密計算システム2が含む秘密計算装置21A, 21B, 21Cの構成を示すブロック図である。また、図8は、秘密計算システム2が含む変換装置20

の構成を示すブロック図である。なお、変換装置 $20_1 \sim 20_N$ を総称して変換装置20と呼ぶ。

[0108] 図6に示すように、秘密計算システム2は、秘密計算装置21A、21B、21C(第1、2、3の秘密計算装置)を有する。

[0109] 図7(A)に示すように、秘密計算装置21Aは、記憶部21AA、入力部21AB、出力部21AC、ビット秘匿部21AE及び秘密計算部21AFを有する。また、図7(B)に示すように、秘密計算装置21Bは、記憶部21BA、入力部21BB、出力部21BC、ビット秘匿部21BD、選択部21BE及び関数秘匿部21BFを有する。また、図7(C)に示すように、秘密計算装置21Cは、記憶部21CA、入力部21CB、出力部21CC、ビット秘匿部21CD及び選択部21CEを有する。また、図8に示すように、変換装置20は、それぞれ、記憶部20A、入力部20B、出力部20C及び分割部20Dを有する。

[0110] なお、秘密計算装置11A、11B、11C、変換装置20の例は、CPU、RAM、ROM、通信装置、入力インタフェース、出力インタフェースなどからなる公知のコンピュータに所定のプログラムが読み込まれて構成された装置である。また、秘密計算装置21A、21B、21C、変換装置20が集積回路を含んでもよい。

[0111] <処理>

本実施形態の処理は、前述した本発明の第1態様の一例である。

本実施形態では、前処理によって、各変換装置 $20_1 \sim 20_N$ の記憶部20Aに、それぞれ入力値 $m_1 \sim m_N$ が格納され、秘密計算装置21Bの記憶部21BAに論理回路関数 $f(x_1, \dots, x_N)$ が格納されている。本実施形態の秘密計算システム2は、各変換装置 $20_1 \sim 20_N$ によって保有された入力値 $m_1 \sim m_N$ が他の装置に知られることなく、入力値 m_n ($1 \leq n \leq N$)を入力とした論理回路関数 $f(x_1, \dots, x_N)$ の演算結果 $f(m_1, \dots, m_N)$ を算出する。その際、各秘密計算装置21A、21B、21Cは、入力値 m_n を復元することなく、また入力値 m_n を容易に復元できるデータを得ることなく、演算結果 $f(m_1, \dots, m_N)$ を求める。

[0112] まず、変換装置 20_1 は、入力値 m_1 を、演算子*に対して $m_1 = s_1 * t_1$ を満たす断片 s_1 と断片 t_1 の2つに分割し、断片 s_1 を秘密計算装置21Bに送信し、断片 t_1 を秘密計算装置21Cに送信する。他の変換装置 $20_2 \sim 20_N$ の動作も変換装置 20_1 と同様である(ス

テップE2-1)。

[0113] 秘密計算装置21Cは、変換装置20₁～20_Nから送信された断片 t_n の各ビットbに対応した各データWbと、各ビットbの各反転ビット(1-b)に対応した各データW(1-b)とを生成する。そして、秘密計算装置21Cの出力部21CCは、ビットb及び反転ビット(1-b)とデータWb及びデータW(1-b)との対応を特定せずに、データWb及びデータW(1-b)を含むデータWを秘密計算装置21Bに送信し、データWbを秘密計算装置21Aに送信する(ステップE2-2)。

[0114] 秘密計算装置21Bは、変換装置20₁～20_Nから送信された断片 s_n と論理回路関数 $f(x_1, \dots, x_N)$ とデータWを用い、論理回路関数 $f(x_1, \dots, x_N)$ に断片 s_n が埋め込まれた論理回路関数 $f(s_1 * X_1, \dots, s_N * X_N)$ が秘匿されたデータTであって、当該データTとデータWbとから、入力値 $m_1 \sim m_N$ に対する論理回路関数 $f(x_1, \dots, x_N)$ の演算結果 $f(m_1, \dots, m_N)$ を求めることができるものを生成する。秘密計算装置21Bは、データTを秘密計算装置21Aに送信する(ステップE2-3)。

[0115] 秘密計算装置21Aには、データTとデータWbとが入力される。秘密計算装置21Aは、データTとデータWbとを用いて演算結果 $f(m_1, \dots, m_N)$ を算出する(ステップE2-4, 5)。

[0116] 以下に、本実施形態の秘密計算システム2の動作の具体例を示す。

図9は、第2の実施形態の秘密計算システム2の動作の具体例を示すシーケンス図である。

[ステップE2-1]

この例では、演算子*としてXORを用いる。各変換装置20₁～20_Nの分割部20Dが、それぞれの記憶部21Aに格納された入力値 m_n を

[0117] [数52]

$$m_n = s_n \oplus t_n$$

となるランダムな断片 s_n, t_n に分割する(ステップS201)。そして、各変換装置20₁～20_Nの出力部20Cが、断片 s_n を秘密計算装置21Bに送信し(ステップS202)、断片 t_n を秘密計算装置21Cにそれぞれ送信する(ステップS203)。

[0118] [ステップE2-2]

秘密計算装置21Cのビット秘匿部21CDは、論理回路関数 $f(s_1 * X_1, \dots, s_N * X_N)$ の $m_n = s_n * X_n$ の X_n に対応する入力ワイヤー i ごとに、固定長の乱数であるデータ W_i^0 とランダムビット c_i との組、及び、固定長の乱数である W_i^1 とランダムビット c_i の反転ビットとの組からなる

[0119] [数53]

$$W_i = (\langle W_i^0, c_i \rangle, \langle W_i^1, \bar{c}_i \rangle)$$

を生成する(「データ W 」の具体例)。

[0120] また、選択部21CEは、上記のように生成された W_i から、実際の t_n の各ビット b' に対応する組

[0121] [数54]

$$\langle W_i^{b'}, b' \oplus c_i \rangle$$

をそれぞれ選択する(ステップS204)。なお、 b' は、入力ワイヤー i への入力断片 t_n の下位 w 番目のビットである場合における、断片 t_n の下位 w 番目のビットを意味する。また、

[0122] [数55]

$$\langle W_i^{b'}, b' \oplus c_i \rangle$$

は「データ Wb 」の具体例である。

[0123] そして、秘密計算装置21Cの出力部21CCは、 W_i を秘密計算装置21Bに送信し(ステップS205)、

[0124] [数56]

$$\langle W_i^{b'}, b' \oplus c_i \rangle$$

を秘密計算装置21Aに送信する(ステップS206)。

[0125] [ステップE2-3]

秘密計算装置21Bが、以下の(a)～(d)を実行することにより、論理回路関数 $f(x_1, \dots, x_N)$ に断片 s_n が埋め込まれた論理回路関数 $f(s_1 * X_1, \dots, s_N * X_N)$ を秘匿する。なお、この例の論理回路関数 $f(x_1, \dots, x_N)$ に断片 s_n が埋め込まれた論理回路関数 $f(s_1 * X_1, \dots, s_N * X_N)$ は、断片 $X = t_n$ を入力として $m_n = s_n * X_n$ を復元する関数 $m_n = s_n$

$s_n * X_n$ と、論理回路関数 $f(x_1, \dots, x_N)$ とを含み、論理回路関数 $f(x_1, \dots, x_N)$ に各関数 $m_n = s_n * X_n$ の出力値 m_n を入力して $f(m_1, \dots, m_N)$ を出力する関数である。以下では、このような論理回路関数 $f(s_1 * X_1, \dots, s_N * X_N)$ を構成する各論理ゲートを秘匿する。

[0126] (a) 秘密計算装置21Bのビット秘匿部21BDが、論理回路関数 $f(s_1 * X_1, \dots, s_N * X_N)$ の各ワイヤー i に対して、固定長の乱数

[0127] [数57]

$$w_i^0, w_i^1$$

を生成し、それぞれ0, 1に対応させる。ただし、関数 $m_n = s_n * X_n$ を構成する論理ゲートのうち、 $X_n = t_n$ のビットが入力される入力ワイヤーに対しては、秘密計算装置21Cから受け取った

[0128] [数58]

$$w_i^0, w_i^1$$

を対応させる。

[0129] (b) 次に、秘密計算装置21Bのビット秘匿部11BDは、ランダムビット c_i を生成する。ただし、関数 $m_n = s_n * X_n$ を構成する論理ゲートのうち、 $X_n = t_n$ のビットが入力される入力ワイヤーに対しては、秘密計算装置11Cから受け取った c_i を用いるため、 $X_n = t_n$ のビットが入力される入力ワイヤーに対しては新たなランダムビット c_i を生成しない。

(c) 更に、秘密計算装置21Bのビット秘匿部21BDは、

[0130] [数59]

$$\langle w_i^0, c_i \rangle, \langle w_i^1, \bar{c}_i \rangle$$

をワイヤー i に対応させる。ただし、 s_n の下位 w 番目のビットに対応するワイヤー i には、

[0131] [数60]

$$\langle w_i^b, b \oplus c_i \rangle, \langle w_i^{\bar{b}}, \bar{b} \oplus c_i \rangle$$

を対応させる。ここで b は s_n の下位 w 番目のビットである。

(d) 更に、秘密計算装置21Bの関数秘匿部21BFが、 i, j を入力ワイヤー、 k を出力ワイヤーとする論理ゲート g に対して、4つのラベル付きデータ

[0132] [数61]

$$c_i, c_j : (W_k^{g(0,0)}, g(0,0) \oplus c_k) \oplus F_{W_i^0}(c_j) \oplus F_{W_j^0}(c_i),$$

$$c_i, \bar{c}_j : (W_k^{g(0,1)}, g(0,1) \oplus c_k) \oplus F_{W_i^0}(\bar{c}_j) \oplus F_{W_j^1}(c_i),$$

$$\bar{c}_i, c_j : (W_k^{g(1,0)}, g(1,0) \oplus c_k) \oplus F_{W_i^1}(c_j) \oplus F_{W_j^0}(\bar{c}_i),$$

$$\bar{c}_i, \bar{c}_j : (W_k^{g(1,1)}, g(1,1) \oplus c_k) \oplus F_{W_i^1}(\bar{c}_j) \oplus F_{W_j^1}(\bar{c}_i),$$

を生成し、それらをランダムな順番に並べたデータ T_g を生成する。 T_g の集合 T_g が論理回路関数 $f(s_1 * X_1, \dots, s_N * X_N)$ を秘匿化したデータとなる(ステップS207)。

[0133] 秘密計算装置B21の出力部21BCは、 T_g の集合 T_g を $f(s_1 * X_1, \dots, s_N * X_N)$ の秘匿化データとして秘密計算装置21Aに送信する(ステップS208)。

[ステップE2-4]

秘密計算装置21Aの入力部21ABには、データ T_g の集合 T_g と

[0134] [数62]

$$\langle W_i^{b'}, b' \oplus c_i \rangle$$

が入力される。秘密計算装置21Aの秘密計算部21AFは、データ T_g と

[0135] [数63]

$$\langle W_i^{b'}, b' \oplus c_i \rangle$$

を用いて、論理回路関数 f の最終段の論理ゲート g のワイヤーの出力

[0136] [数64]

$$\langle W_i^{\hat{b}}, \hat{b} \oplus c_i \rangle$$

を得る。

[0137] [ステップE2-5]

秘密計算装置21Aの秘密計算部21AFは、

[0138] [数65]

$$\langle W_i^{\hat{b}}, \hat{b} \oplus c_i \rangle$$

から、演算結果 $f(m_1, \dots, m_N)$ のビット

[0139] [数66]

$$\hat{b}$$

を得る(ステップS209)。

[0140] 以上、説明したように、本実施形態によれば、非特許文献3の技術を用いた秘密計

算システムでは全体の計算量の大部分を占めていた、proxy 1-out-of-2 Oblivious Transferプロトコルを秘密計算装置21A, 21B, 21Cのいずれも実行する必要がないので、秘密計算装置21A, 21B, 21Cの負荷を大幅に低減することができる。

- [0141] なお、本実施形態で追加された秘密計算装置21Cには入力値 m_n の断片 t_n が与えられるだけなので、秘密計算装置21Cによって入力値 m_n の秘匿性が損なわれることはない。

また、本実施形態では、XORを演算子*として用いる例を示したが、本発明はこれに限定されるものではない。例えば、加減算、乗算、その他どのような演算子を演算子*としてもよい。

- [0142] また、本実施形態では、各変換装置 $20_1 \sim 20_N$ によって分割された各断片 t_n が秘密計算装置21Cに送信される構成であった(ステップS203)。しかし、各変換装置 $20_1 \sim 20_N$ によって分割された各断片 t_n が、まず、秘密計算装置21Aに送信され、そこから秘密計算装置21Cに転送される構成であってもよい。また、各変換装置 $20_1 \sim 20_N$ によって分割された各断片 t_n が、秘密計算装置21Aに送信され、本実施形態のステップS204, S205の処理を秘密計算装置21Aが実行する構成であってもよい。これらの場合であっても、断片 t_n と断片 s_n とが秘匿されることなく同一の秘密計算装置に入力されることはないため、入力値 m_n の秘匿性が損なわれることはない。

- [0143] また、本実施形態では、断片 t_n が入力された秘密計算装置21Cがデータ W_i を生成し、生成したデータ W_i を秘密計算装置21Bに送信する構成とした。しかし、秘密計算装置21Bがデータ W_i を生成し、生成したデータ W_i を秘密計算装置21Cに送信する構成であってもよい。

- [0144] [第3の実施形態]

本実施形態の秘密計算システムは、N個(Nは正の整数)の変換装置と2つの秘密計算装置とからなる。各変換装置はそれぞれ互いに独立な入力値を保持している。本実施形態の秘密計算システムは、各変換装置によって保有された入力値が他の装置に知られることなく、それらの入力値に対する論理回路関数fの演算結果を算出する。

[0145] <構成>

図10は、第3の実施形態の秘密計算システム3の構成を示すブロック図である。また、図11(A)(B)は、秘密計算システム3が含む秘密計算装置31A, 31Bの構成を示すブロック図である。

[0146] 図10に示すように、秘密計算システム3は、変換装置 $20_1 \sim 20_N$ 及び秘密計算装置31A, 31B(第1, 2の秘密計算装置)を有する。図11(A)に示すように、秘密計算装置31Aは、記憶部31AA、入力部31AB、出力部31AC、ビット秘匿部31AD、選択部31AE、関数秘匿部31AF及び1-out-of-2 OT実行部31AGを有する。また、図11(B)に示すように、秘密計算装置31Bは、記憶部31BA、入力部31BB、出力部31BC及び秘密計算部31BFを有する。秘密計算部31BFは1-out-of-2 OT実行部31BFAを含む。なお、変換装置 $20_1 \sim 20_N$ の構成は、第2の実施形態で説明したものと同様である(図8)。

[0147] なお、秘密計算装置31A, 31Bの例は、CPU、RAM、ROM、通信装置、入力インタフェース、出力インタフェースなどからなる公知のコンピュータに所定のプログラムが読み込まれて構成された装置である。また、秘密計算装置31A, 31Bが集積回路を含んでもよい。

[0148] <処理>

本実施形態の処理は、前述した本発明の第2態様の一例である。本実施形態では、前処理によって、各変換装置 $20_1 \sim 20_N$ の記憶部20Aに、それぞれ入力値 $m_1 \sim m_N$ が格納され、秘密計算装置31Aの記憶部31AAに論理回路関数 $f(x_1, \dots, x_N)$ が格納されている。本実施形態の秘密計算システム3は、各変換装置 $20_1 \sim 20_N$ によって保有された入力値 $m_1 \sim m_N$ が他の装置に知られることなく、入力値 m_n ($1 \leq n \leq N$)を入力とした論理回路関数 $f(x_1, \dots, x_N)$ の演算結果 $f(m_1, \dots, m_N)$ を算出する。その際、各秘密計算装置31A, 31Bは、入力値 m_n を復元することなく、また入力値 m_n を容易に復元できるデータを得ることなく、演算結果 $f(m_1, \dots, m_N)$ を求める。

[0149] まず、変換装置 20_1 は、入力値 m_1 を、演算子*に対して $m_1 = s_1 * t_1$ を満たす断片 s_1 と断片 t_1 の2つに分割し、断片 t_1 を秘密計算装置31Aに送信し、断片 s_1 を秘密計算装置31Bに送信する。他の変換装置 $20_2 \sim 20_N$ の動作も変換装置 20_1 と同様である(ス

テップE3-1)。

[0150] 秘密計算装置31Aは、論理回路関数 $f(x)$ と変換装置 $20_1 \sim 20_N$ から送信された断片 t_n とを用い、論理回路関数 $f(x)$ に断片 t_n が埋め込まれた論理回路関数 $f(X_{1_1} * t_{1_1}, \dots, X_{N_N} * t_{N_N})$ が秘匿されたデータTであって、当該データTと断片 s_n とから演算結果 $f(m_{1_1}, \dots, m_{N_N})$ を求めることのできるものを生成する。秘密計算装置31Aは、データTを秘密計算装置31Bに送信する(ステップE3-2)。

[0151] 秘密計算装置31Bには、断片 s_n とデータTとが入力される。秘密計算装置31Bは、断片 s_n とデータTとを用いて演算結果 $f(m_{1_1}, \dots, m_{N_N})$ を算出する。秘密計算装置31Bは、断片 s_n を入力として、入力値 m_n を実際に復元することなく、データTから演算結果 $f(m_{1_1}, \dots, m_{N_N})$ を算出する(ステップE3-3、4、5)。

[0152] 以下に、本実施形態の秘密計算システム3の動作の具体例を示す。

図12は、第3の実施形態の秘密計算システム3の動作の具体例を示すシーケンス図である。

[ステップE3-1]

各変換装置 $20_1 \sim 20_N$ の分割部20Dが、それぞれの記憶部21Aに格納された入力値 m_n を

[0153] [数67]

$$m_n = s_n \oplus t_n$$

となるランダムな断片 s_n, t_n に分割する(ステップS301)。そして、各変換装置 $20_1 \sim 20_N$ の出力部20Cが、断片 s_n を秘密計算装置31Bに送信し(ステップS302)、断片 t_n を秘密計算装置31Aにそれぞれ送信する(ステップS303)。

[0154] [ステップE3-2]

秘密計算装置31Aは、以下の(a)～(d)を実行することにより、論理回路関数 $f(x_{1_1}, \dots, x_{N_N})$ に断片 t_n が埋め込まれた論理回路関数 $f(X_{1_1} * t_{1_1}, \dots, X_{N_N} * t_{N_N})$ を秘匿する。なお、この例の論理回路関数 $f(x_{1_1}, \dots, x_{N_N})$ に断片 t_n が埋め込まれた論理回路関数 $f(X_{1_1} * t_{1_1}, \dots, X_{N_N} * t_{N_N})$ は、断片 $X = s_n$ を入力として $m_n = X * t_n$ を復元する関数 $m_n = X * t_n$ と、論理回路関数 $f(x_{1_1}, \dots, x_{N_N})$ とを含み、論理回路関数 $f(x_{1_1}, \dots, x_{N_N})$ に各関数 $m_n = X * t_n$ の出力値 m_n を入力して $f(m_{1_1}, \dots, m_{N_N})$ を出力する関数である。

以下では、このような論理回路関数 $f(X_{11}^{*t}, \dots, X_{NN}^{*t})$ を構成する各論理ゲートを秘匿する。

[0155] (a) 秘密計算装置31Aのビット秘匿部31ADが、論理回路関数 $f(s_{11}^{*X}, \dots, s_{NN}^{*X})$ を構成する各論理ゲートの各ワイヤー i に対して、固定長の乱数

[0156] [数68]

$$W_i^0, W_i^1$$

を生成し、それぞれ0, 1に対応させる。

[0157] (b) 秘密計算装置31Aのビット秘匿部31ADは、ランダムビット $c_i \in \{0, 1\}$ を生成する。

(c) 秘密計算装置31Aのビット秘匿部31ADは、

[0158] [数69]

$$(\langle W_i^0, c_i \rangle, \langle W_i^1, \bar{c}_i \rangle)$$

をワイヤー i に対応させる。ただし、断片 t_n の下位 w 番目のビットに対応する入力ワイヤー i には、

[0159] [数70]

$$(\langle W_i^{b_w}, b_w \oplus c_i \rangle, \langle W_i^{\bar{b}_w}, b_w \oplus \bar{c}_i \rangle)$$

を対応させる。ここで b_w は、断片 t_n の下位 w 番目のビットである。

[0160] (d) 秘密計算装置31Aの関数秘匿部31AFが、 i, j を入力ワイヤー、 k を出力ワイヤーとする論理ゲート g に対して、4つのラベル付きデータ

[0161] [数71]

$$\begin{aligned} c_i, c_j : (W_k^{g(0,0)}, g(0,0) \oplus c_k) \oplus F_{W_i^0}(c_j) \oplus F_{W_j^0}(c_i), \\ c_i, \bar{c}_j : (W_k^{g(0,1)}, g(0,1) \oplus c_k) \oplus F_{W_i^0}(\bar{c}_j) \oplus F_{W_j^1}(c_i), \\ \bar{c}_i, c_j : (W_k^{g(1,0)}, g(1,0) \oplus c_k) \oplus F_{W_i^1}(c_j) \oplus F_{W_j^0}(\bar{c}_i), \\ \bar{c}_i, \bar{c}_j : (W_k^{g(1,1)}, g(1,1) \oplus c_k) \oplus F_{W_i^1}(\bar{c}_j) \oplus F_{W_j^1}(\bar{c}_i), \end{aligned}$$

を生成し、それらをランダムな順番に並べたデータ T_g を生成する。 T_g の集合 T が論理回路関数 $f(X_{11}^{*t}, \dots, X_{NN}^{*t})$ を秘匿化したデータとなる(ステップS304)。

[0162] 秘密計算装置31Aの出力部31ACは、 T_g の集合 T を論理回路関数 $f(X_{11}^{*t}, \dots, X_{NN}^{*t})$ の秘匿化データとして秘密計算装置31Bに送信する(ステップS305)。

[ステップE3-3]

秘密計算装置31Bの入力部31BBには、各変換装置20₁ ~ 20_N から送信された断片s_nが入力されている。秘密計算装置31Bの秘密計算部31BDは、これらの断片s_nを用い、断片s_nの各ビットbに対応する

[0163] [数72]

$$\langle w_i^b, b \oplus c_i \rangle$$

を求める。しかしながら、 w_i^b や c_i は秘密計算装置31Aで設定されたものであり、秘密計算装置31Bのみでは、断片s_nの各ビットbに対応する w_i^b や c_i を設定できない。一方、断片s_nの各ビットbに対応する w_i^b や c_i を秘密計算装置31Aから得るために、秘密計算装置31Aに断片s_nの各ビットbの情報を与えたのでは、秘密計算装置31Aに入力値m_nが復元されてしまう。よって、秘密計算装置31Bの秘密計算部31BDが具備する1-out-of-2 OT実行部31BDAは、秘密計算装置31Aの1-out-of-2 OT実行部31AGとの間で1-out-of-2 Oblivious Transferプロトコルを実行し、秘密計算装置31Aに断片s_nの各ビットbの情報を与えることなく、秘密計算装置31Aから断片s_nの各ビットbに対応する w_i^b や c_i を取得する。以下、この処理の一例を示す。

[0164] [1-out-of-2 Oblivious Transferプロトコルの例]

《パラメータ設定》

1-out-of-2 OT実行部31BDAと1-out-of-2 OT実行部31AGとは、協力して素数pを生成し、 $h^q \equiv 1 \pmod{p}$ を満たす2以上p未満の整数hおよび最小の自然数qを求める。また、これらは、別に2以上p未満の整数zを選ぶ。このように設定された素数p、自然数q、整数h、整数zは、例えば、秘密計算装置31Aの記憶部31AAと秘密計算装置31Bの記憶部31BAとに格納される。

[0165] 《秘密鍵設定》

1-out-of-2 OT実行部31BDAが、q未満の自然数uをランダムに選ぶ。この自然数uは秘密鍵である。

[0166] 《公開鍵設定》

1-out-of-2 OT実行部31BDAが、q未満の自然数uをランダムに選ぶ。この

自然数 u は秘密鍵である。 $PK_b = h^u \bmod p$ を計算する。この PK_b は公開鍵であり、秘密鍵 u で暗号化された暗号文は PK_b によって正しく復号できる。

[0167] 《公開鍵の改変》

1-out-of-2 OT実行部31BDAは、 $b=1$ であれば

[0168] [数73]

$$PK_{\bar{b}} = z / PK_b \bmod p$$

を計算する。

[0169] 《公開鍵の送信》

秘密計算装置31Bの出力部31BCは、 PK_0 を秘密計算装置31Aに送信する。なお、 $b=0$ であれば PK_0 は自然数 u に対応する正しい公開鍵である。一方、 $b=1$ であれば PK_0 は自然数 u に対応する正しい公開鍵ではなく、かつ、 $PK_1 = z / PK_0 \bmod p$ によって得られる PK_1 が自然数 u に対応する正しい公開鍵となる。

[0170] 《暗号化》

秘密計算装置31Aの1-out-of-2 OT実行部31AGは、送信された PK_0 を用いて $PK_1 = z / PK_0 \bmod p$ を計算した後、

[0171] [数74]

$$Z_0 = E_{PK_0}(C(W_i^0, c_i)) \quad Z_1 = E_{PK_1}(C(W_i^1, c_i))$$

[0172] を計算する。秘密計算装置31Aの出力部31ACは、得られた暗号文 Z_0, Z_1 を秘密計算装置31Bに送信する。ここで $E_{PK}(x)$ は平文 x の公開鍵 PK を用いた暗号化関数であるとし、その暗号文は復号鍵 u により復号できるものとする。また C は平文が正しく復元できたか識別可能な関数である。なお、秘密計算装置31Aは、 PK_0 及び PK_1 の何れが自然数 u に対応する正しい公開鍵であることを知ることはできない。そのため、秘密計算装置31Aは、秘密計算装置31Aがビット $b=0$ に対応するデータを取得しようとしているのか、ビット $b=1$ に対応するデータを取得しようとしているのかを知ることができない。

[0173] 《復号》

秘密計算装置31Bの1-out-of-2 OT実行部31BDAは、復号鍵 u を用いて Z_0, Z_1 を復号し、正しく復元されていると C により識別される復号結果

[0174] [数75]

$$\langle w_i^b, b \oplus c_i \rangle$$

を得る。すなわち、 $b=0$ であれば PK_0 が自然数 u に対応する正しい公開鍵であるため Z_0 のみが正しく復元され、 $b=1$ であれば PK_1 が自然数 u に対応する正しい公開鍵であるため Z_1 のみが正しく復元される(ステップS306)。

[0175] [ステップE3-4]

秘密計算装置31Bの入力部31BBには、データ T_g の集合 T と

[0176] [数76]

$$\langle w_i^b, b \oplus c_i \rangle$$

が入力される。秘密計算装置31Bの秘密計算部31BDは、 T_g および

[0177] [数77]

$$\langle w_i^b, b \oplus c_i \rangle$$

を用いて、論理回路関数 f の最終段の論理ゲート g のワイヤーの出力

[0178] [数78]

$$\langle w_i^{\hat{b}}, \hat{b} \oplus c_i \rangle$$

を得る。

[0179] [ステップE3-5]

秘密計算装置31Bの秘密計算部31BDは、

[0180] [数79]

$$\langle w_i^{\hat{b}}, \hat{b} \oplus c_i \rangle$$

から、演算結果 $f(m_1, \dots, m_N)$ のビット

[0181] [数80]

$$\hat{b}$$

を得る(ステップS307)。

[0182] 本実施形態によれば、変換装置 $20_1 \sim 20_N$ は、保有しているデータ m_n を s_n と t_n に分割し、 s_n を秘密計算装置31Bに送り、 t_n を秘密計算装置31Aに送るだけでよく、proxy 1-out-of-2 Oblivious Transferプロトコルを実行する必要はない。よって

、これが必要な非特許文献3に開示された方法に比べて、変換装置201～20Nの負荷が低減される。

[0183] なお、本実施形態では、秘密計算装置31Bが、ステップS306で、断片 s_n の各ビット b に対応するデータとして、各ビット b の秘匿データ

[0184] [数81]

$$\langle w_i^b, b \oplus c_i \rangle$$

を取得する例を示した。

[0185] しかし、秘密計算装置31Bが、断片 s_n の各ビット b に対応するデータとして、入力値 $m_n = s_n * t_n$ の各ビット r に対応する秘匿データを取得する構成であってもよい。このような構成は、例えば、演算子 $*$ がXORであるならば、上述の Z_0, Z_1 の代わりに以下の Z_0, Z_1 を用いることで実現できる。なお、 v は断片 t_n のビットを示す。

[0186] [数82]

$$Z_0 = E_{PK_0}(C(\langle w_i^v, v \oplus c_i \rangle)) \quad Z_1 = E_{PK_1}(C(\langle w_i^{\bar{v}}, \bar{v} \oplus c_i \rangle))$$

[0187] これは、断片 s_n のビット b が0であれば、それと同じ桁の入力値 $m_n = s_n * t_n$ のビット r は、それと同じ桁の断片 t_n のビット v と等しくなるし、断片 s_n のビット b が1であれば、それと同じ桁の入力値 $m_n = s_n * t_n$ のビット r は、それと同じ桁の断片 t_n のビット v の反転ビットとなることに基づく。この場合、秘密計算装置31Bは、

[0188] [数83]

$$\begin{aligned} &\langle w_i^v, v \oplus c_i \rangle \quad (b=0) \\ &\langle w_i^{\bar{v}}, \bar{v} \oplus c_i \rangle \quad (b=1) \end{aligned}$$

の何れかを得る。これに応じたデータ T_g の集合 T が設定してあれば、これらから演算結果 $f(m_1, \dots, m_N)$ の演算結果を得ることができる。

[0189] また、本実施形態では、XORを演算子 $*$ として用いる例を示したが、本発明はこれに限定されるものではない。例えば、加減算、乗算、その他どのような演算子を演算子 $*$ としてもよい。

[0190] [第4の実施形態]

本実施形態の秘密計算システムは、 N 個(N は正の整数)の変換装置と2つの秘密計算装置とからなる。各変換装置はそれぞれ互いに独立な入力値を保持している。

本実施形態の秘密計算システムは、各変換装置によって保有された入力値が他の装置に知られることなく、それらの入力値に対する論理回路関数 f の演算結果を算出する。ただし、本実施形態では、1-out-of-2 Oblivious Transferプロトコルを用いない。

[0191] <構成>

図13は、第4の実施形態の秘密計算システム4の構成を示すブロック図である。また、図14(A)(B)は、秘密計算システム4が含む秘密計算装置41A, 41Bの構成を示すブロック図である。また、図15は、秘密計算システム4が含む変換装置 $40_1 \sim 40_N$ の構成を示すブロック図である。なお、変換装置 $40_1 \sim 40_N$ を総称して変換装置40と呼ぶ。

[0192] 図13に示すように、秘密計算システム4は、変換装置 $40_1 \sim 40_N$ 及び秘密計算装置41A, 41B(第1, 2の秘密計算装置)を有する。図14(A)に示すように、秘密計算装置41Aは、記憶部41AA、入力部41AB、出力部41AC、ビット秘匿部41AD及び関数秘匿部41AFを有する。また、図14(B)に示すように、秘密計算装置41Bは、記憶部41BA、入力部41BB、出力部41BC及び秘密計算部41BFを有する。また、図15示すように、変換装置40は、記憶部40A、入力部40B、出力部40C、ビット秘匿部40D及び選択部40Eを有する。

[0193] なお、秘密計算装置41A, 41B及び変換装置40の例は、CPU、RAM、ROM、通信装置、入力インタフェース、出力インタフェースなどからなる公知のコンピュータに所定のプログラムが読み込まれて構成された装置である。また、秘密計算装置31A, 31B及び変換装置40が集積回路を含んでもよい。

[0194] <処理>

本実施形態の処理は、前述した本発明の第2態様の一例である。本実施形態では、前処理によって、各変換装置 $40_1 \sim 40_N$ の記憶部40Aに、それぞれ入力値 $m_1 \sim m_N$ が格納され、秘密計算装置41Aの記憶部41AAに論理回路関数 $f(x_1, \dots, x_N)$ が格納されている。本実施形態の秘密計算システム4は、各変換装置 $40_1 \sim 40_N$ に保有された入力値 $m_1 \sim m_N$ が他の装置に知られることなく、入力値 m_n ($1 \leq n \leq N$)を入力とした論理回路関数 $f(x_1, \dots, x_N)$ の演算結果 $f(m_1, \dots, m_N)$ を算出する。その際

、各秘密計算装置41A、41Bは、入力値 m_n を復元することなく、また入力値 m_n を容易に復元できるデータを得ることなく、演算結果 $f(m_1, \dots, m_N)$ を求める。また、これらの処理の過程で1-out-of-2 Oblivious Transferプロトコルを実行する必要はない。

[0195] まず、変換装置 $40_1 \sim 40_N$ が、各入力値 $m_1 \sim m_N$ の各ビット b に対応したデータ Wb と、各ビット b に対する反転ビット $(1-b)$ に対応したデータ $W(1-b)$ とを生成する。そして、変換装置 $40_1 \sim 40_N$ は、各入力値 $m_1 \sim m_N$ を分割した一方の断片としてデータ Wb を秘密計算装置41Bに送信する。また、変換装置 $40_1 \sim 40_N$ は、データ Wb と各ビット b の反転ビット $(1-b)$ に対応した各データ $W(1-b)$ とを、データ Wb 及びデータ $W(1-b)$ と b 及び $(1-b)$ との対応を特定せずに含むデータ W を他方の断片として秘密計算装置41Aに送信する(ステップE4-1)。

[0196] 秘密計算装置41Aは、データ W を用い、論理回路関数 f が秘匿されたデータ T であって当該データ T とデータ Wb とを用いて演算結果 $f(m)$ を求めることのできるものを生成する。秘密計算装置41Aは、生成したデータ T を秘密計算装置41Bに送信する(ステップE4-2)。

[0197] 秘密計算装置11Aには、データ T とデータ Wb とが入力される。秘密計算装置11Aは、データ T とデータ Wb とを用いて演算結果 $f(m)$ を算出する(ステップE4-3, 4, 5)。

[0198] 以下に、本実施形態の秘密計算システム4の動作の具体例を示す。

図16は、第4の実施形態の秘密計算システム4の動作の具体例を示すシーケンス図である。

[ステップE4-1]

各変換装置 $40_1 \sim 40_N$ のビット秘匿部40Dが、論理回路関数 $f(x_1, \dots, x_N)$ を構成する各論理ゲートのうち、各入力値 $m_1 \sim m_N$ のビット b が入力される各入力ワイヤー i に対して、ランダムビット c_i 及び固定長の乱数

[0199] [数84]

$$w_i^0, w_i^1$$

を生成する。そして、各変換装置 40_n の秘匿部40Dは、

$$W_n = (c_i, W_i^0, W_i^1)$$

を生成し(データWの例/ステップS401)、各変換装置40_nの選択部40Eは、各ビットbに対応する

[0200] [数85]

$$\langle W_i^b, b \oplus c_i \rangle_n$$

を生成する(データWbの例/ステップS402)。各変換装置40_nの出力部40CはW_nを秘密計算装置41Bに送信し(ステップS403)、

[0201] [数86]

$$\langle W_i^b, b \oplus c_i \rangle_n$$

を秘密計算装置41Aに送信する(ステップS404)。

[0202] [ステップE4-2]

秘密計算装置41Aの関数秘匿部41AFは、上述したステップE3-2と同様に、(a)～(d)を実行することにより、論理回路関数 $f(x_1, \dots, x_N)$ を構成する各論理ゲートが秘匿されたT_gの集合Tを生成する。ただし、入力値 $m_1 \sim m_N$ の各ビットの入力ワイヤーiには、

[0203] [数87]

$$(\langle W_i^0, c_i \rangle, \langle W_i^1, \bar{c}_i \rangle)$$

を対応させる(ステップS405)。

[0204] 秘密計算装置41Aの出力部41ACは、T_gの集合Tを論理回路関数 $f(x_1, \dots, x_N)$ の秘匿化データとして秘密計算装置41Bに送信する(ステップS406)。

[ステップE4-3]

秘密計算装置41Bの入力部41BFには、データT_gの集合Tと

[0205] [数88]

$$\langle W_i^b, b \oplus c_i \rangle_n$$

が入力される。秘密計算装置41Bの秘密計算部41BFは、T_gおよび

[0206] [数89]

$$\langle W_i^b, b \oplus c_i \rangle_n$$

を用いて、論理回路関数 f の最終段の論理ゲート g のワイヤーの出力

[0207] [数90]

$$\langle w_i^b, \hat{b} \oplus c_i \rangle$$

を得る。

[0208] [ステップE4-5]

秘密計算装置41Bの秘密計算部41BDは、

[0209] [数91]

$$\langle w_i^b, \hat{b} \oplus c_i \rangle$$

から、演算結果 $f(m_1, \dots, m_N)$ のビット

[0210] [数92]

$$\hat{b}$$

を得る(ステップS407)。

[0211] この例によれば、1-out-of-2 Oblivious Transferプロトコルを実行する必要が無いので、第3の実施形態と比べて、秘密計算装置41A、41Bの処理が軽減される。

また、各変換装置40_nから秘密計算装置41Aに送信される

$$W_n = (c_i, W_i^0, W_i^1)$$

には、入力値 m_n に関する情報が含まれていない。また、各変換装置40_nから秘密計算装置41Bに送信される

[0212] [数93]

$$\langle w_i^b, b \oplus c_i \rangle_n$$

[0213] は、入力値 m_n のビット b がランダムビット c_i でマスクされているため、入力値 m_n に関する有意な情報とはならない。したがって、秘密計算装置41A、41Bは自身の受信した情報からだけでは、入力値 m_n に関する有意な情報を得ることができず、入力値 m_n の秘匿性が確保される。

[0214] [変形例等]

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、入力値や

断片が埋め込まれた論理回路関数の構成方法は上述のものには限定されない。また、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。また、本明細書においてシステムとは、複数の装置の論理的集合構成である。また、各装置の構成が同一筐体内にあるとは限らない。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。

[0215] また、上述の構成をコンピュータによって実現する場合、各装置が有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。

この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等のようなものでもよい。

[0216] また、このプログラムの流通は、例えば、そのプログラムを記録したDVD、CD-R OM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。

[0217] このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理の実行時、このコンピュータは、自己の記録媒体に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。また、サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるASP (Application Service Pro

vider)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。

産業上の利用可能性

[0218] 本発明は、例えば、プライバシーを保護しつつ個人的な情報を活用する様々なシステムに適用できる。例えば、本発明は、オークションを含む任意の情報集計システムに利用できる。この場合、各ユーザーが保有するデータを漏洩させることなく、オークション結果や多数決による意思決定の結果などを演算結果として得ることができる。また、本発明の他の適用例は、例えば、各ユーザーが保有するデータを他者に知られること無く集計し、それらのデータを元にした各種統計処理やマイニング処理を行うシステムである。更に他の例として、本発明を生体認証システムに利用することも可能である。この場合には、各ユーザーの生体情報が秘匿されたままで、生体情報が正当なものであるかを否か判定できる。

請求の範囲

- [1] 第1の入力値mAが秘匿されたままで、当該第1の入力値mAに対する論理回路関数fの演算結果f(mA)を算出する秘密計算システムであって、
- 第1の秘密計算装置と、前記論理回路関数fを格納した第2の秘密計算装置と、第3の秘密計算装置とを有し、
- 前記第3の秘密計算装置は、
- 前記第1の入力値mA及び演算子*に対して $mA = s * t$ を満たす断片tの各ビットbに対応した各データWbと、前記各ビットbの各反転ビット(1-b)に対応した各データW(1-b)とを生成する手段と、
- 前記データWbを前記第1の秘密計算装置に送信する手段と、
- 前記ビットb及び反転ビット(1-b)と前記データWb及び前記データW(1-b)との対応を特定せずに、前記データWb及び前記データW(1-b)を含むデータWを前記第2の秘密計算装置に送信する手段と、を含み、
- 前記第2の秘密計算装置は、
- $mA = s * t$ を満たす断片sと前記論理回路関数fと前記データWとを用い、前記論理回路関数fに前記断片sが埋め込まれた論理回路関数f(s*X)が秘匿されたデータTであって、当該データTと前記データWbとから前記演算結果f(mA)を求めることができるものを生成する手段と、
- 前記データTを前記第1の秘密計算装置に送信する手段と、を含み、
- 前記第1の秘密計算装置は、
- 前記データTと前記データWbとが入力される手段と、
- 前記データTと前記データWbとを用いて前記演算結果f(mA)を算出する手段と、を含む。
- [2] 請求項1の秘密計算システムであって、
- 前記第1の秘密計算装置は、
- 前記第1の入力値mAを格納する手段と、
- 前記第1の入力値mAを、 $mA = s * t$ を満たす前記断片s, tに分割する手段と、
- 前記断片sを前記第2の秘密計算装置に送信する手段と、

- 前記断片 t を前記第3の秘密計算装置に送信する手段と、を含む。
- [3] 請求項1又は2の秘密計算システムであって、
- 前記論理回路関数 f は、2つの入力値を入力とする論理回路関数 $f(x, y)$ であり、
- 前記第2の秘密計算装置は、第2の入力値 mB を格納する手段を含み、
- 前記データ T を生成する手段は、前記断片 s と前記論理回路関数 $f(x, y)$ と前記データ W と前記入力値 mB を用い、前記論理回路関数 $f(x, y)$ に前記断片 s と前記入力値 mB とが埋め込まれた論理回路関数 $f(s * X, mB)$ が秘匿されたデータ T であって、当該データ T と前記データ Wb とから前記第1の入力値 mA 及び前記第2の入力値 mB に対する前記論理回路関数 $f(x, y)$ の演算結果 $f(mA, mB)$ を求めることができるものを生成する手段を含み、
- 前記演算結果 $f(mA)$ を算出する手段は、
- 前記データ T と前記データ Wb とを用いて前記演算結果 $f(mA, mB)$ を算出する手段を含む。
- [4] 請求項1の秘密計算システムであって、
- 前記第1の入力値 mA を、 $mA = s * t$ を満たす前記断片 s, t に分割する手段と、
- 前記断片 s を前記第2の秘密計算装置に送信する手段と、
- 前記断片 t を前記第3の秘密計算装置に送信する手段と、を含む変換装置を更に有する。
- [5] 秘密計算装置であって、
- 1の入力値 mA 及び演算子 $*$ に対して $mA = s * t$ を満たす断片 t が入力される手段と、
- 、
- 前記断片 t の各ビット b に対応した各データ Wb と、前記各ビット b の各反転ビット $(1 - b)$ に対応した各データ $W(1 - b)$ とを生成する手段と、
- 前記データ Wb を、前記第1の入力値 mA に対する論理回路関数 f の演算結果 $f(mA)$ を算出する他の秘密計算装置に送信する手段と、
- 前記ビット b 及び反転ビット $(1 - b)$ と前記データ Wb 及び前記データ $W(1 - b)$ との対応を特定せずに、前記データ Wb 及び前記データ $W(1 - b)$ を含むデータ W を、 $mA = s * t$ を満たす断片 s が入力された他の秘密計算装置に送信する手段と、を有する

- 。
- [6] 秘密計算装置であって、
- 1の入力値mA及び演算子*に対して $mA = s * t$ を満たす断片sが入力される手段と、
- 、
- 前記断片sと論理回路関数fとデータWとを用い、当該論理回路関数fに前記断片sが埋め込まれた論理回路関数 $f(s * X)$ が秘匿されたデータTであって、当該データTと前記データWbとから前記第1の入力値mAに対する前記論理回路関数fの演算結果 $f(mA)$ を求めることができるものを生成する手段と、
- 前記データTを、前記演算結果 $f(mA)$ を算出する他の秘密計算装置に送信する手段と、を有する。
- [7] 第1、第2、及び第3の秘密計算装置により、第1の入力値mAが秘匿されたままで、当該第1の入力値mAに対する論理回路関数fの演算結果 $f(mA)$ を算出する秘密計算方法であって、
- (A) 前記第3の秘密計算装置において、前記第1の入力値mA及び演算子*に対して $mA = s * t$ を満たす断片tの各ビットbに対応した各データWbと、前記各ビットbの各反転ビット $(1 - b)$ に対応した各データ $W(1 - b)$ とを生成するステップと、
- (B) 前記第3の秘密計算装置において、前記データWbを前記第1の秘密計算装置に送信するステップと、
- (C) 前記第3の秘密計算装置において、前記ビットb及び反転ビット $(1 - b)$ と前記データWb及び前記データ $W(1 - b)$ との対応を特定せずに、前記データWb及び前記データ $W(1 - b)$ を含むデータWを前記第2の秘密計算装置に送信するステップと、
- 、
- (D) 前記第2の秘密計算装置において、 $mA = s * t$ を満たす断片sと当該第2の秘密計算装置に格納された前記論理回路関数fと前記データWとを用い、前記論理回路関数fに前記断片sが埋め込まれた論理回路関数 $f(s * X)$ が秘匿されたデータTであって、当該データTと前記データWbとから前記演算結果 $f(mA)$ を求めることができるものを生成するステップと、
- (E) 前記第2の秘密計算装置において、前記データTを前記第1の秘密計算装置

に送信するステップと、

(F) 前記第1の秘密計算装置に前記データTと前記データWbとが入力されるステップと、

(G) 前記第1の秘密計算装置において、前記データTと前記データWbとを用いて前記演算結果 $f(mA)$ を算出するステップと、を有する。

[8] 請求項7の秘密計算方法であって、

前記第1の秘密計算装置において、当該第1の秘密計算装置に格納された前記第1の入力値 mA を、 $mA = s * t$ を満たす前記断片 s , t に分割するステップと、

前記断片 s を前記第2の秘密計算装置に送信するステップと、

前記断片 t を前記第3の秘密計算装置に送信するステップと、を有する。

[9] 請求項7又は8の秘密計算方法であって、

前記論理回路関数 f は、2つの入力値を入力とする論理回路関数 $f(x, y)$ であり、

前記第2の秘密計算装置には、第2の入力値 mB が格納されており、

前記ステップ(D)は、前記断片 s と前記論理回路関数 $f(x, y)$ と前記データWと前記入力値 mB とを用い、前記論理回路関数 f に前記断片 s と前記入力値 mB とが埋め込まれた論理回路関数 $f(s * X, mB)$ が秘匿されたデータTであって、当該データTと前記データWbとから前記第1の入力値 mA 及び前記第2の入力値 mB に対する前記論理回路関数 $f(x, y)$ の演算結果 $f(mA, mB)$ を求めることができるものを生成するステップを含み、

前記ステップ(G)は、前記第1の秘密計算装置において、前記データTと前記データWbとを用いて前記演算結果 $f(mA, mB)$ を算出するステップを含む。

[10] 入力値 m が秘匿にされたままで、当該入力値 m に対する論理回路関数 $f(x)$ の演算結果 $f(m)$ を算出する秘密計算システムであって、

前記論理回路関数 $f(x)$ を格納した第1の秘密計算装置と、第2の秘密計算装置とを有し、

前記第1の秘密計算装置は、

前記入力値 m から分割された断片Aと断片Bとのうち断片Bが入力される手段と、

前記論理回路関数 $f(x)$ と前記断片Bとを用い、前記論理回路関数 $f(x)$ が秘匿され

たデータTであって、当該データTと前記断片Aとから前記演算結果 $f(m)$ を求めることのできるものを生成する手段と、を含み、

前記第2の秘密計算装置は、

前記断片Aと前記データTとが入力される手段と、

前記断片Aと前記データTとを用いて前記演算結果 $f(m)$ を算出する手段と、を含む。

[11] 請求項10の秘密計算システムであって、

前記断片A、Bは、演算子*に対して $mA = s * t$ を満たす断片s, tであり、

前記データTを生成する手段は、前記論理回路関数 $f(x)$ と前記断片tとを用い、前記論理回路関数 $f(x)$ に前記断片tが埋め込まれた論理回路関数 $f(X * t)$ が秘匿されたデータTであって、当該データTと前記断片sとから前記演算結果 $f(m)$ を求めることのできるものを生成する手段を含み、

前記断片Aと前記データTとを用いて前記演算結果 $f(m)$ を算出する手段は、前記断片sと前記データTとを用いて前記演算結果 $f(m)$ を算出する手段を含む。

[12] 請求項11の秘密計算システムであって、

前記断片Aと前記データTとを用いて前記演算結果 $f(m)$ を算出する手段は、前記入力値mを復元することなく、前記断片sと前記データTとを用いて前記演算結果 $f(m)$ を算出する手段を含む。

[13] 請求項12の秘密計算システムであって、

前記断片Aと前記データTとを用いて前記演算結果 $f(m)$ を算出する手段は、

前記第1の秘密計算装置との間で1-out-of-2 Oblivious Transferプロトコルを実行し、前記断片sを前記第1の秘密計算装置に知られることなく、前記断片sに対応する前記第1の秘密計算装置で設定された秘匿データを取得する手段と、

前記秘匿データと前記データTとを用いて前記演算結果 $f(m)$ を算出する手段と、を含む手段である。

[14] 請求項11の秘密計算システムであって、

前記断片Aと前記データTとを用いて前記演算結果 $f(m)$ を算出する手段は、

前記第1の秘密計算装置との間で1-out-of-2 Oblivious Transferプロトコ

ルを実行し、前記断片sを前記第1の秘密計算装置に知られることなく、前記断片sに対応する前記第1の秘密計算装置で設定された秘匿データを取得する手段と、

前記秘匿データと前記データTとを用いて前記演算結果 $f(m)$ を算出する手段と、を含む手段である。

- [15] 請求項11から14の何れかの秘密計算システムであって、
前記入力値 m を、 $m = s * t$ を満たす前記断片 s , t に分割する手段と、
前記断片 t を前記第1の秘密計算装置に送信する手段と、
前記断片 s を前記第2の秘密計算装置に送信する手段と、
を含む変換装置を更に有する。
- [16] 請求項10の秘密計算システムであって、
前記断片Aは、前記入力値 m の各ビット b に対応した各データ W_b であり、
前記断片Bは、前記データ W_b と前記各ビット b の反転ビット $(1-b)$ に対応した各データ $W(1-b)$ とを、前記データ W_b 及び前記データ $W(1-b)$ と b 及び $(1-b)$ との対応を特定せずに含むデータ W であり、
前記データTを生成する手段は、前記データ W を用い、論理回路関数 f が秘匿されたデータTであって当該データTと前記データ W_b とを用いて前記演算結果 $f(m)$ を求めることのできるものを生成する手段を含み、
前記断片Aと前記データTとを用いて前記演算結果 $f(m)$ を算出する手段は、前記データ W_b と前記データTとを用いて前記演算結果 $f(m)$ を算出する手段を含む。
- [17] 秘密計算装置であって、
入力値 m から分割された断片Aと断片Bとのうち断片Bが入力される手段と、
論理回路関数 $f(x)$ と前記断片Bとを用い、前記論理回路関数 $f(x)$ が秘匿されたデータTであって、当該データTと前記断片Aとから前記演算結果 $f(m)$ を求めることのできるものを生成する手段と、
前記断片Aが入力された他の秘密計算装置に前記データTを送信する手段と、を有する。
- [18] 入力値 m が秘匿にされたままで、当該入力値 m に対する論理回路関数 $f(x)$ の演算結果 $f(m)$ を算出する秘密計算方法であって、

(A) 前記第1の秘密計算装置に、前記入力値 m から分割された断片Aと断片Bとのうち断片Bが入力されるステップと、

(B) 前記第1の秘密計算装置において、当該第1の秘密計算装置が格納した前記論理回路関数 $f(x)$ と前記断片Bとを用い、前記論理回路関数 $f(x)$ が秘匿されたデータ T であって、当該データ T と前記断片Aとから前記演算結果 $f(m)$ を求めることのできるものを生成するステップと、

(C) 前記第2の秘密計算装置に、前記断片Aと前記データ T とが入力されるステップと、

(D) 前記第2の秘密計算装置において、前記断片Aと前記データ T とを用いて前記演算結果 $f(m)$ を算出するステップと、を有する。

[19] 請求項18の秘密計算方法であって、

前記断片A、Bは、演算子 $*$ に対して $mA = s * t$ を満たす断片 s , t であり、

前記ステップ(B)は、前記論理回路関数 $f(x)$ と前記断片 t とを用い、前記論理回路関数 $f(x)$ に前記断片 t が埋め込まれた論理回路関数 $f(X * t)$ が秘匿されたデータ T であって、当該データ T と前記断片 s とから前記演算結果 $f(m)$ を求めることのできるものを生成するステップを含み、

前記ステップ(D)は、前記断片 s と前記データ T とを用いて前記演算結果 $f(m)$ を算出するステップを含む。

[20] 請求項18の秘密計算方法であって、

前記ステップ(D)は、前記入力値 m を復元することなく、前記断片 s と前記データ T とを用いて前記演算結果 $f(m)$ を算出するステップを含む。

[21] 請求項20の秘密計算方法であって、

前記ステップ(D)は、

(D-1) 前記第2の秘密計算装置が前記第1の秘密計算装置との間で1-out-of-2 Oblivious Transferプロトコルを実行し、前記断片 s を前記第1の秘密計算装置に知られることなく、前記断片 s に対応する前記第1の秘密計算装置で設定された秘匿データを取得するステップと、

(D-2) 前記秘匿データと前記データ T とを用いて前記演算結果 $f(m)$ を算出するス

テップと、を含む。

[22] 請求項19の秘密計算方法であって、

前記ステップ(D)は、

(D-1) 前記第2の秘密計算装置が前記第1の秘密計算装置との間で1-out-of-2 Oblivious Transferプロトコルを実行し、前記断片sを前記第1の秘密計算装置に知られることなく、前記断片sに対応する前記第1の秘密計算装置で設定された秘匿データを取得するステップと、

(D-2)前記秘匿データと前記データTとを用いて前記演算結果 $f(m)$ を算出するステップと、を含む。

[23] 請求項19から22の何れかの秘密計算方法であって、

変換装置において、前記入力値mを、 $m=s*t$ を満たす前記断片s, tに分割するステップと、

前記変換装置において、前記断片tを前記第1の秘密計算装置に送信するステップと、

前記変換装置において、前記断片sを前記第2の秘密計算装置に送信するステップと、を更に有する。

[24] 請求項19の秘密計算方法であって、

前記断片Aは、前記入力値mの各ビットbに対応した各データ W_b であり、

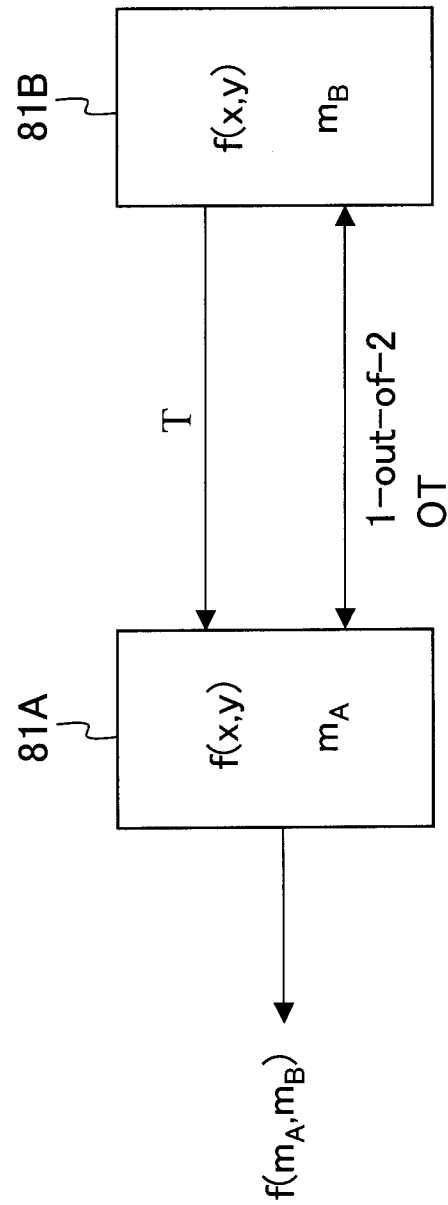
前記断片Bは、前記データ W_b と前記各ビットbの反転ビット $(1-b)$ に対応した各データ $W(1-b)$ とを、前記データ W_b 及び前記データ $W(1-b)$ とb及び $(1-b)$ との対応を特定せずに含むデータWであり、

前記ステップ(B)は、前記データWを用い、論理回路関数fが秘匿されたデータTであって当該データTと前記データ W_b とを用いて前記演算結果 $f(m)$ を求めることのできるものを生成するステップを含み、

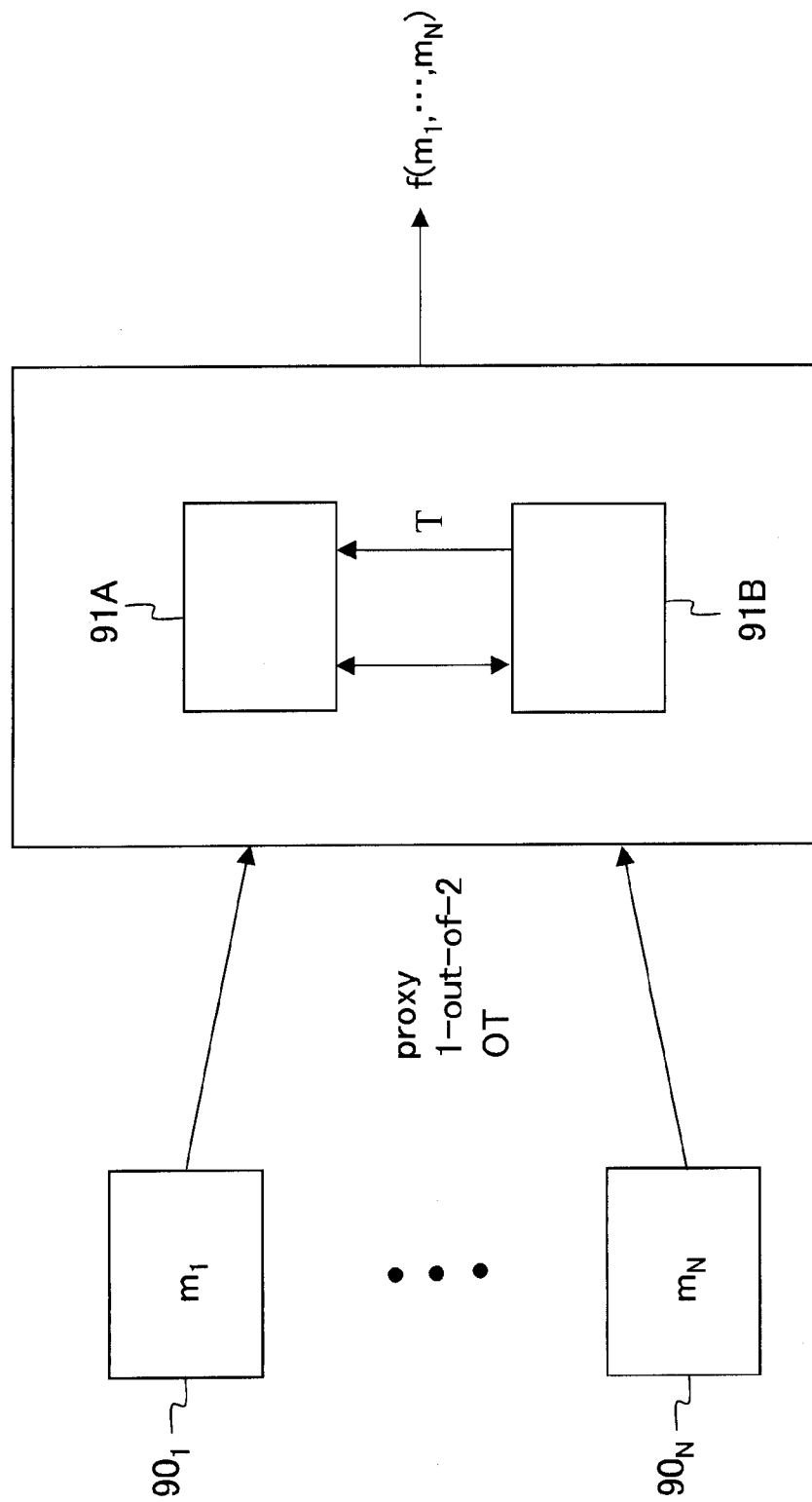
前記ステップ(D)は、前記データ W_b と前記データTとを用いて前記演算結果 $f(m)$ を算出するステップを含む。

[25] 請求項5、6、17の何れかの秘密計算装置としてコンピュータを機能させるためのプログラム。

[図1]



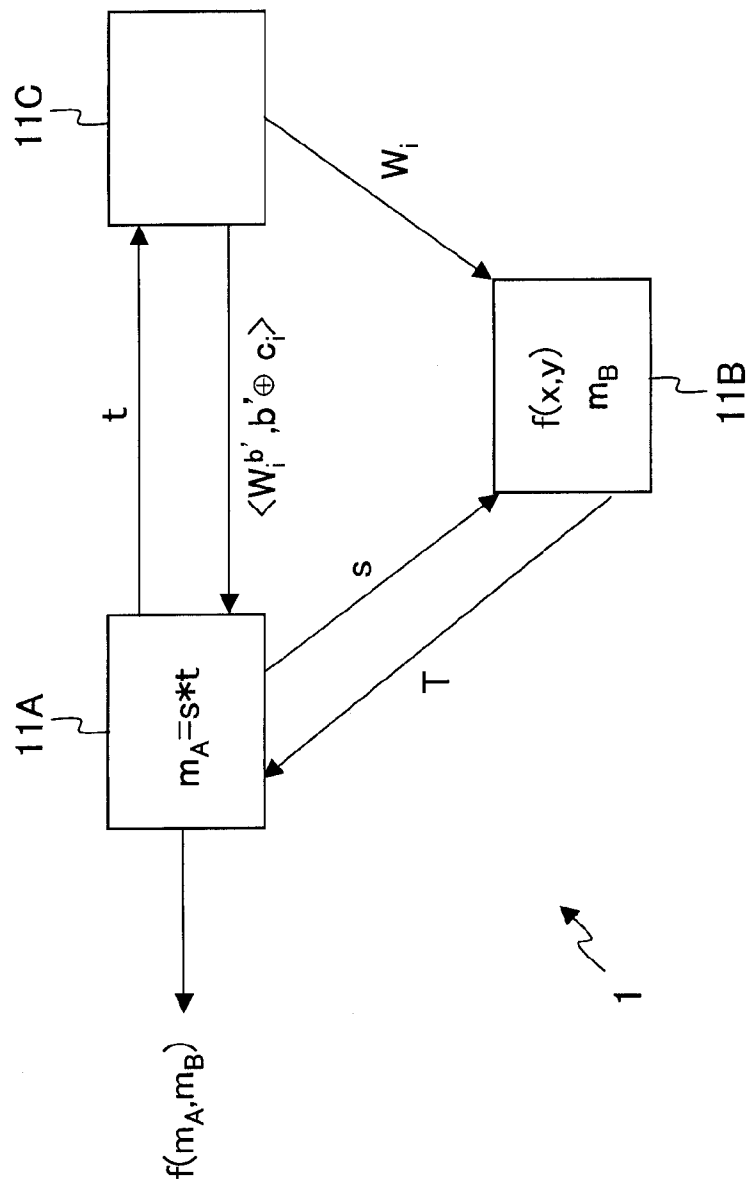
[図2]



[図2]

[図3]

図3



[図4]

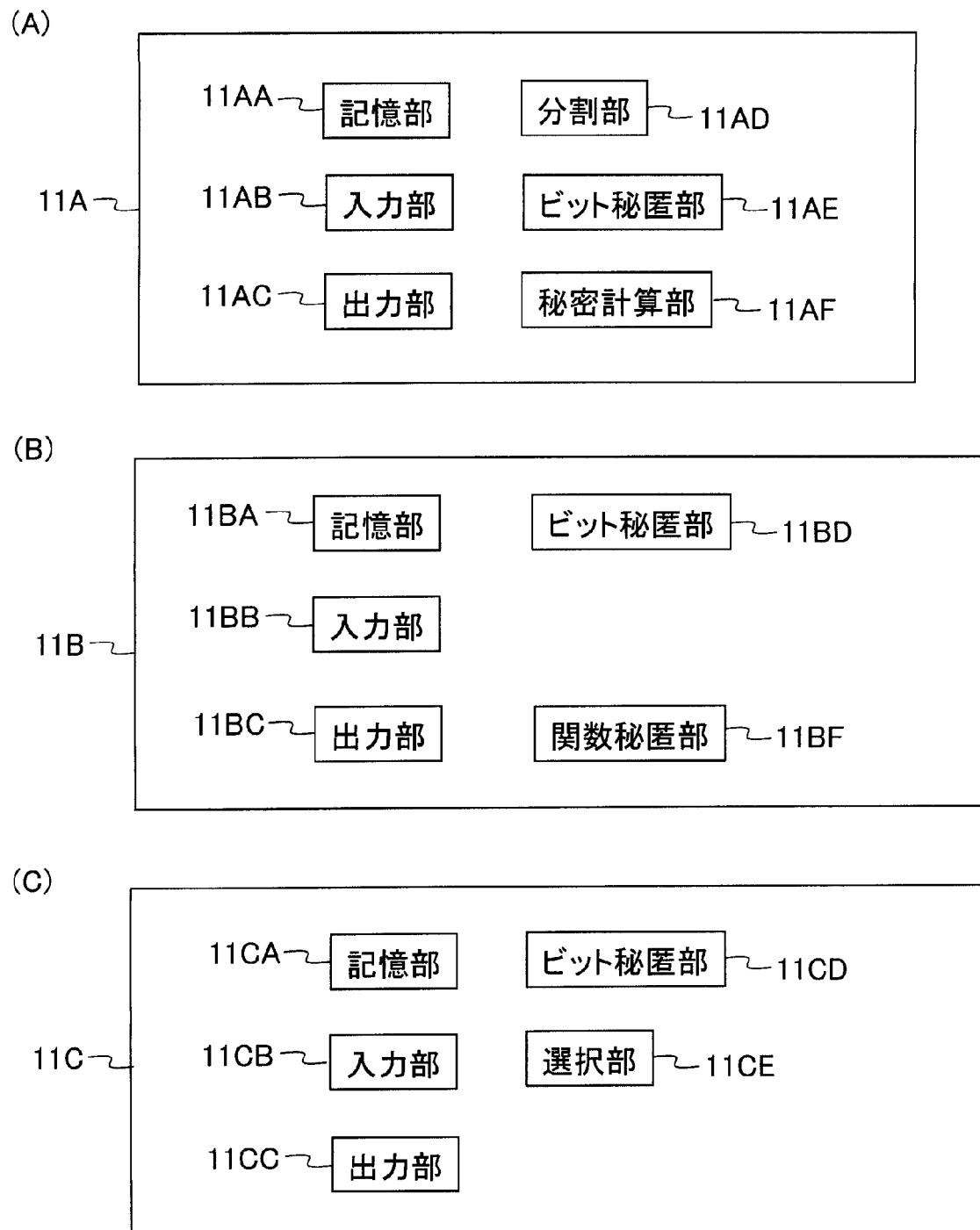


図4

[図5]

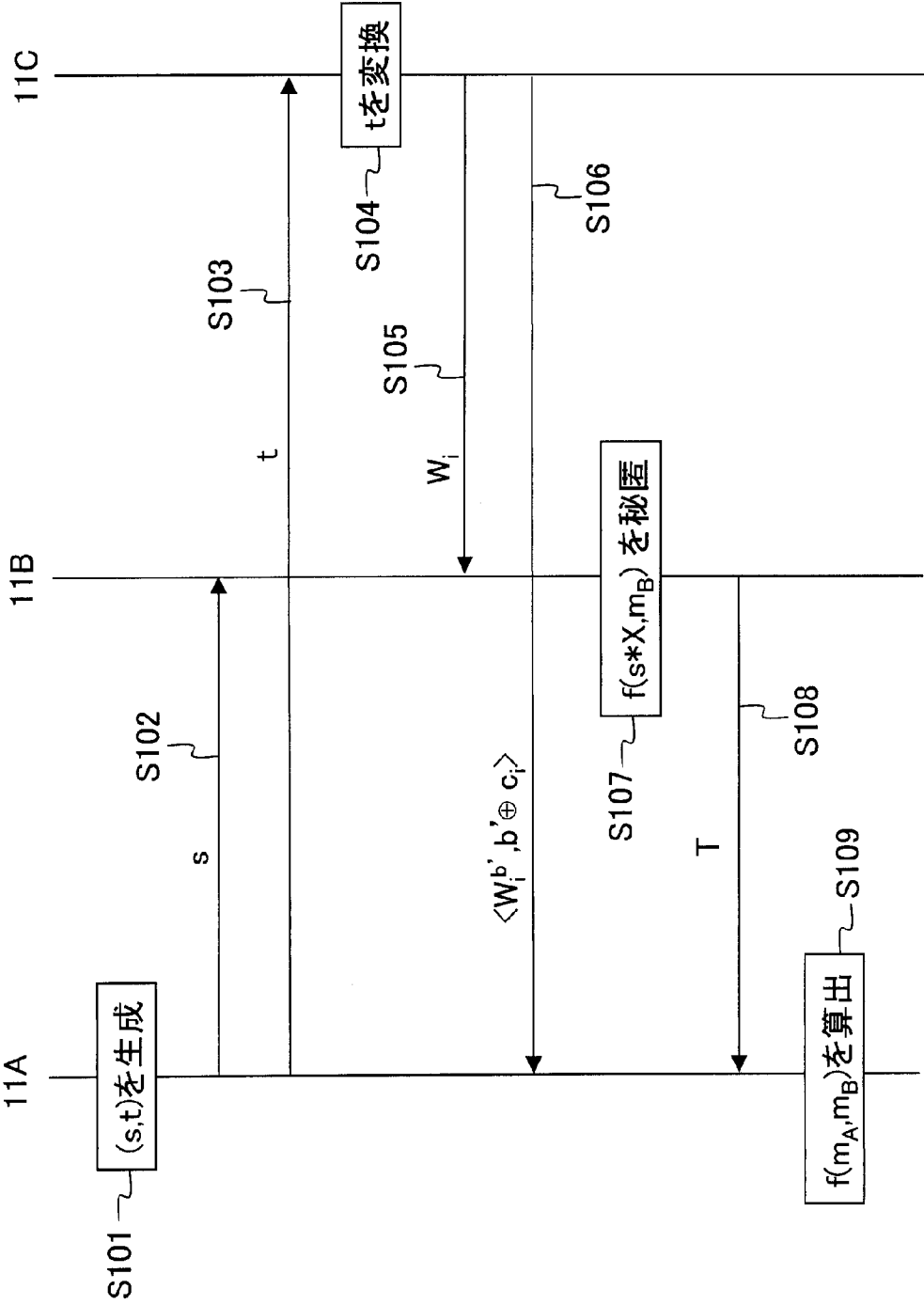
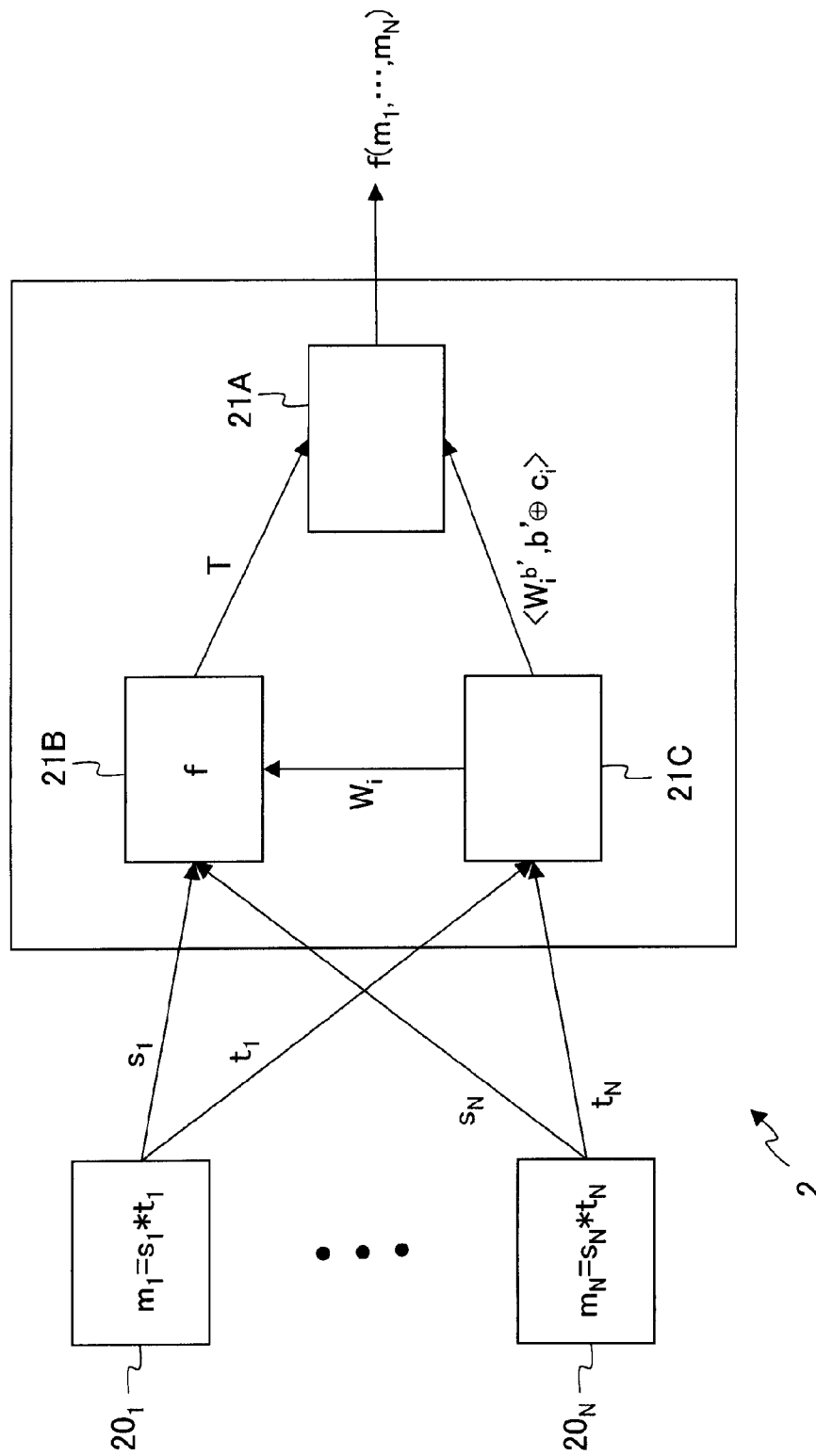


図5

[図6]



[図6]

[図7]

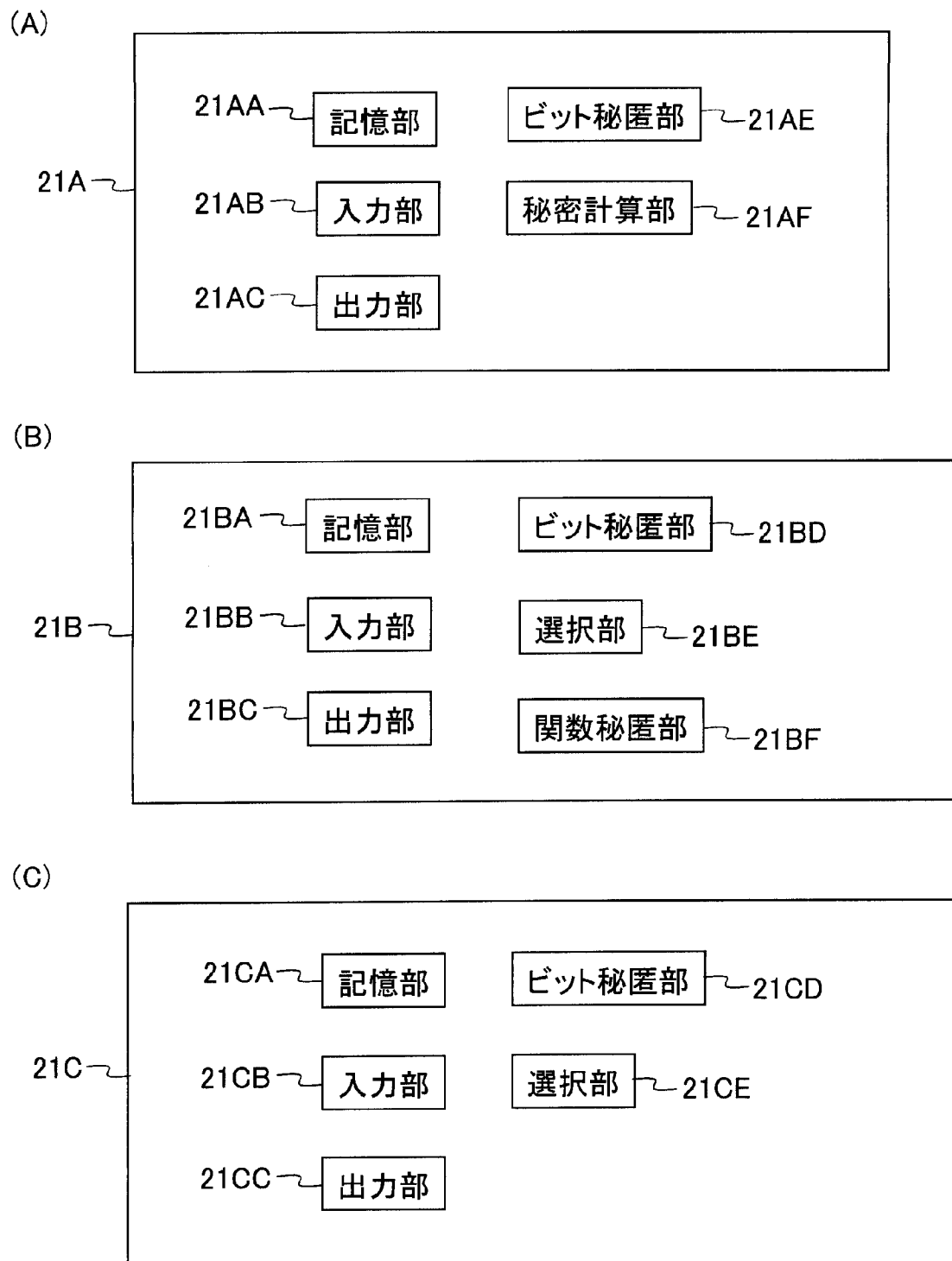


図7

[図8]

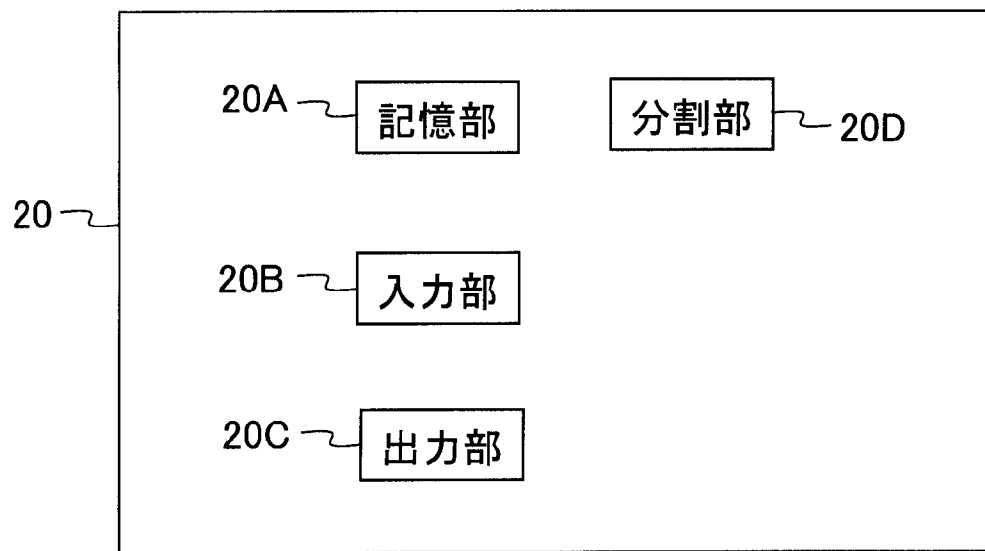


図8

[図9]

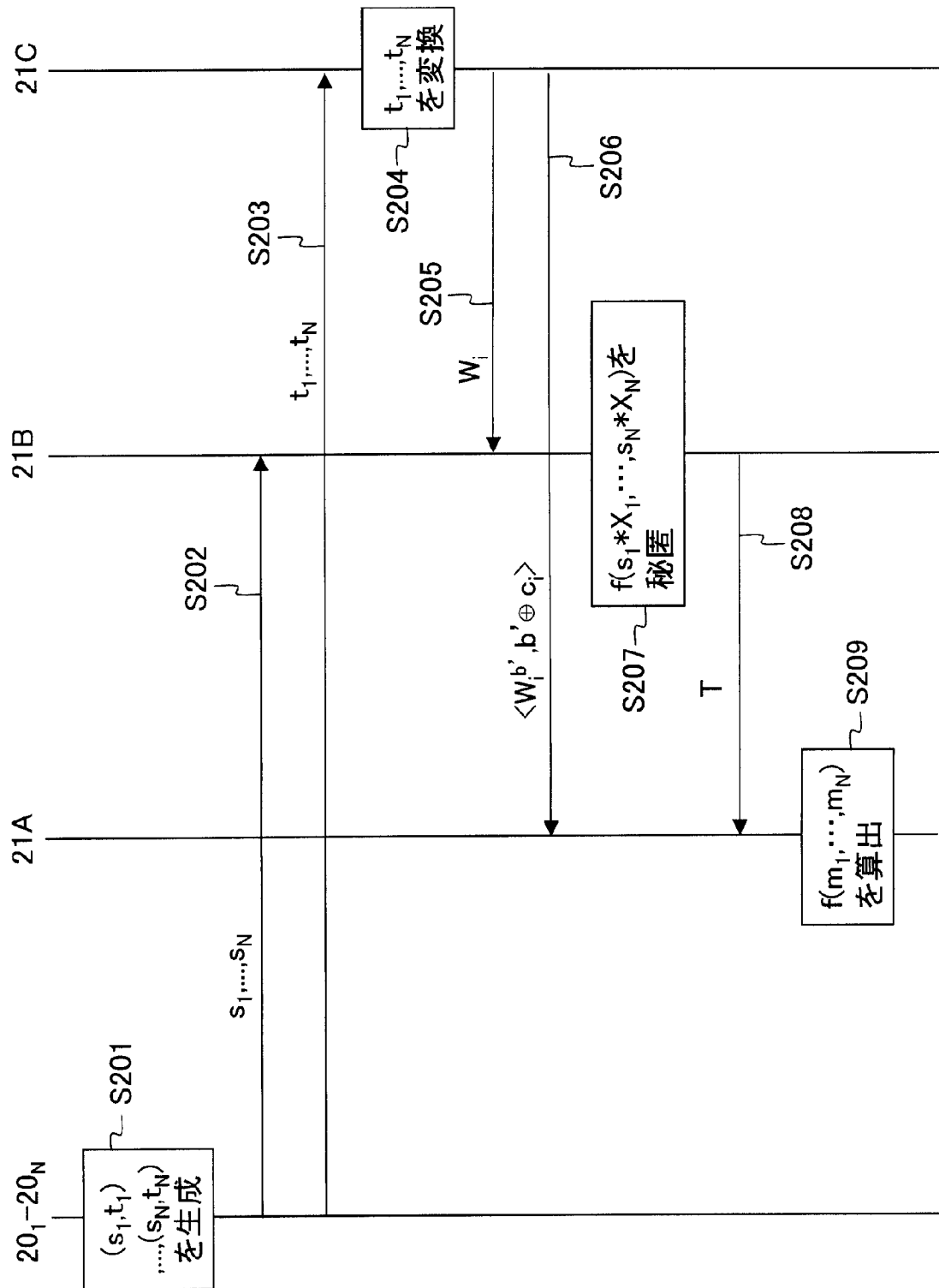


図9

[図10]

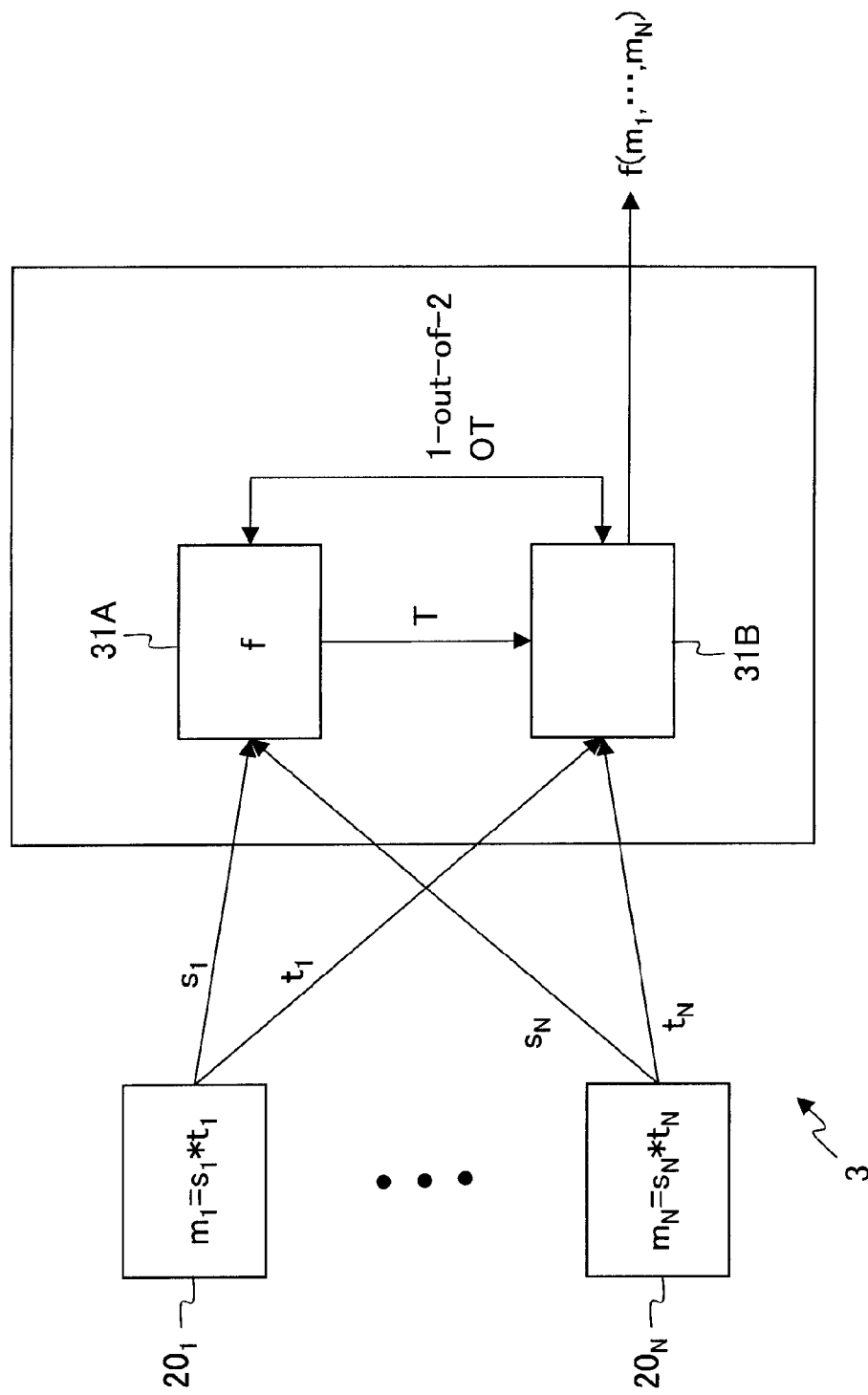


図10

[図11]

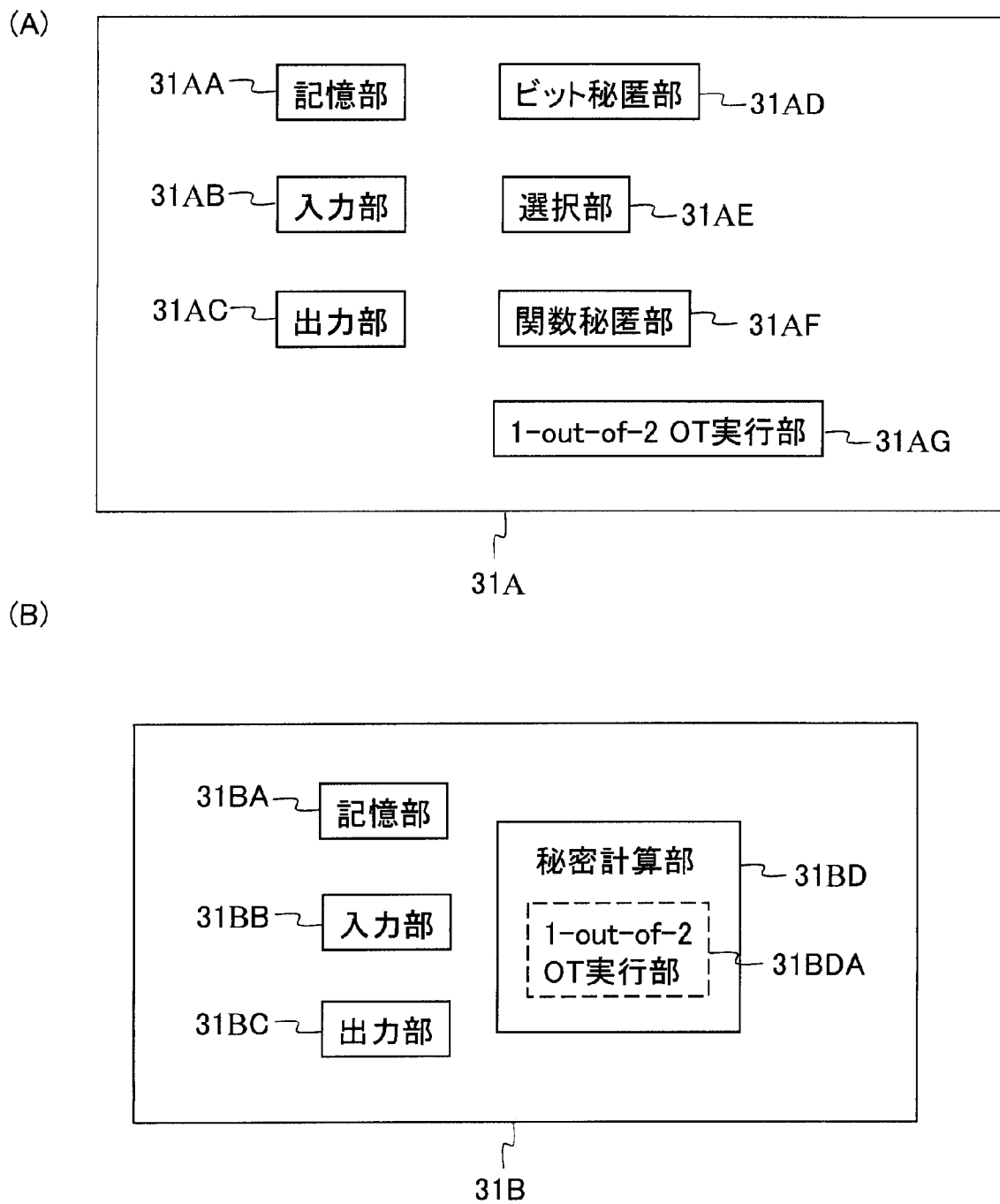


図11

[図12]

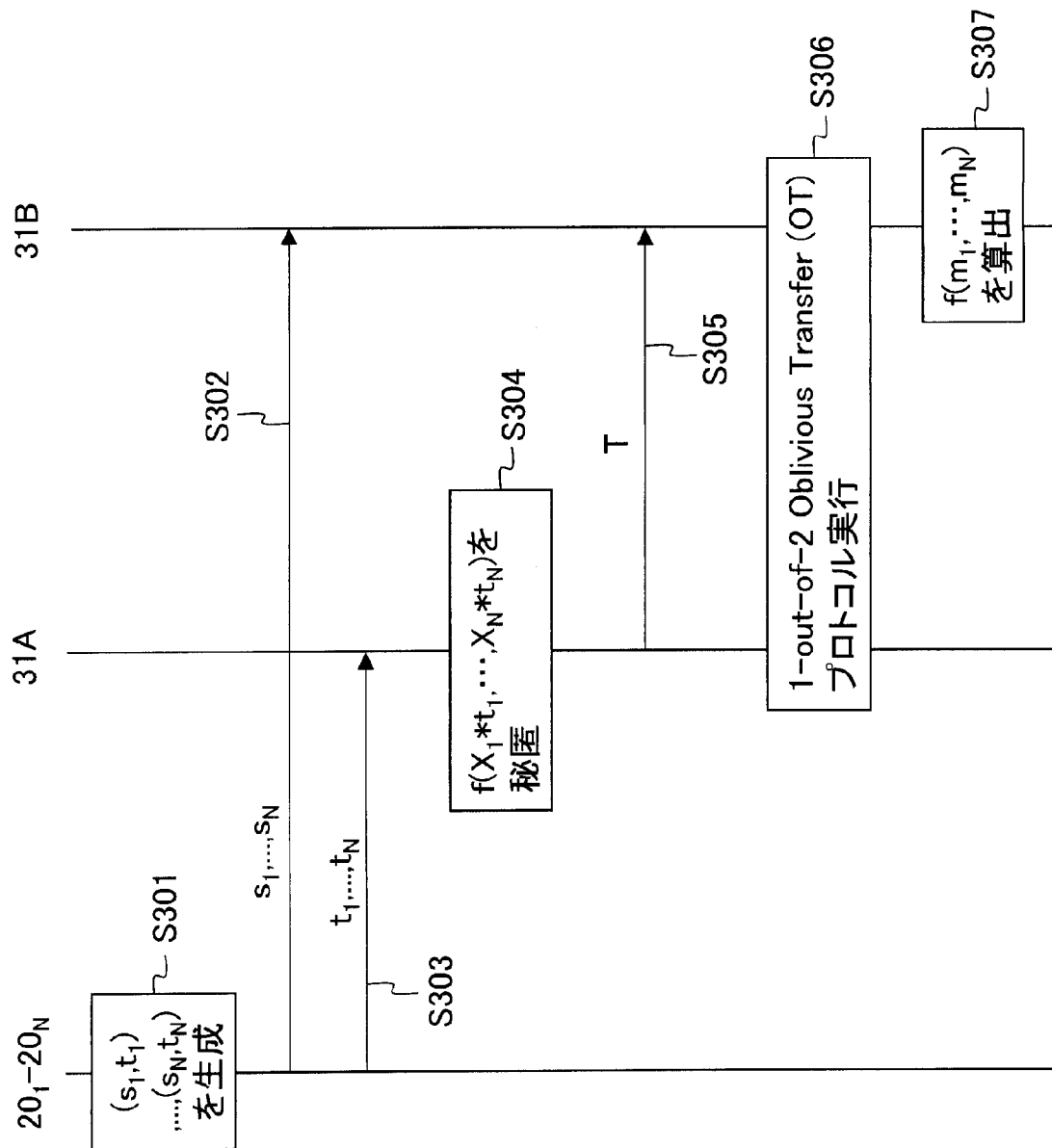


図12

[図13]

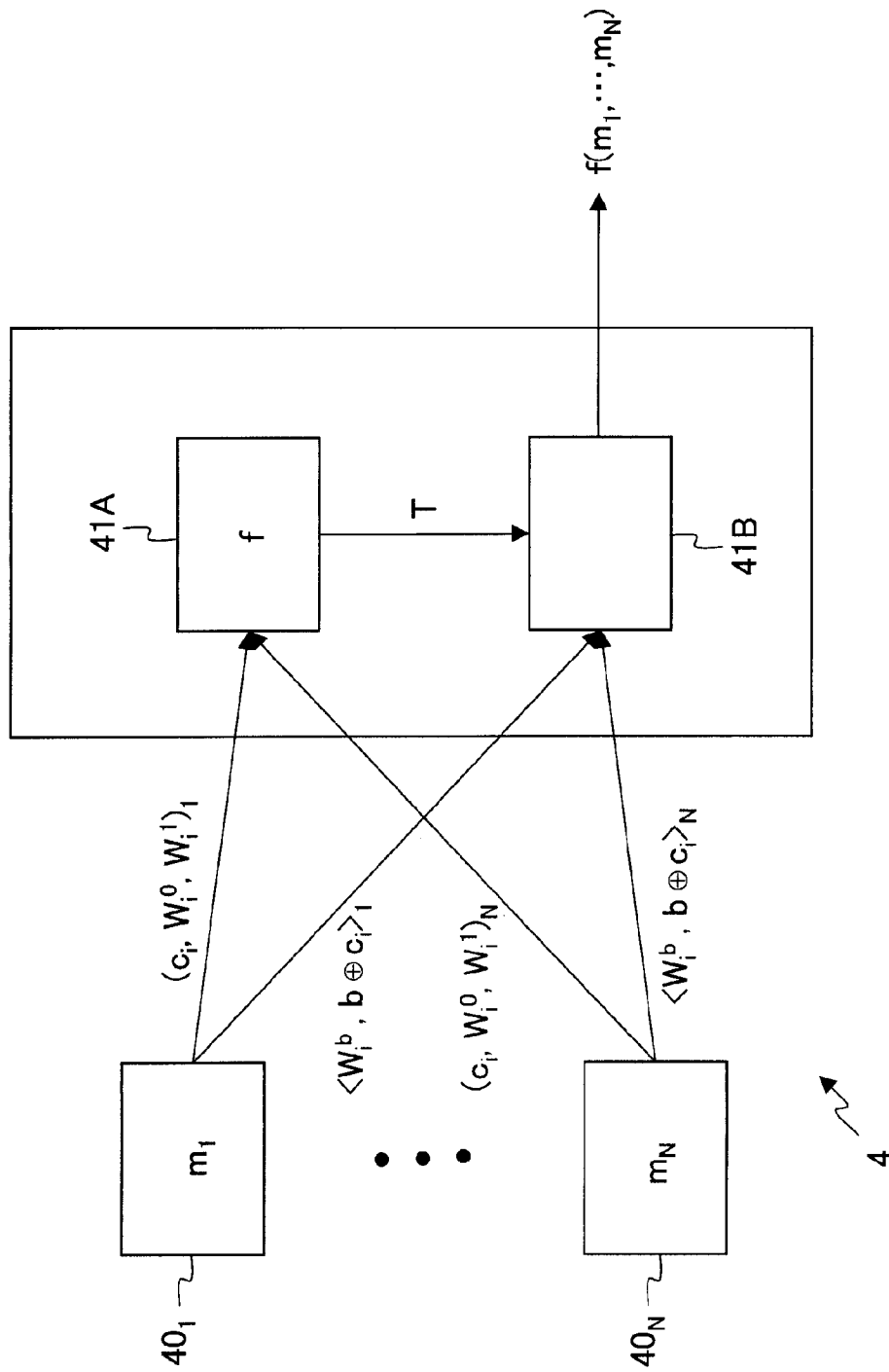
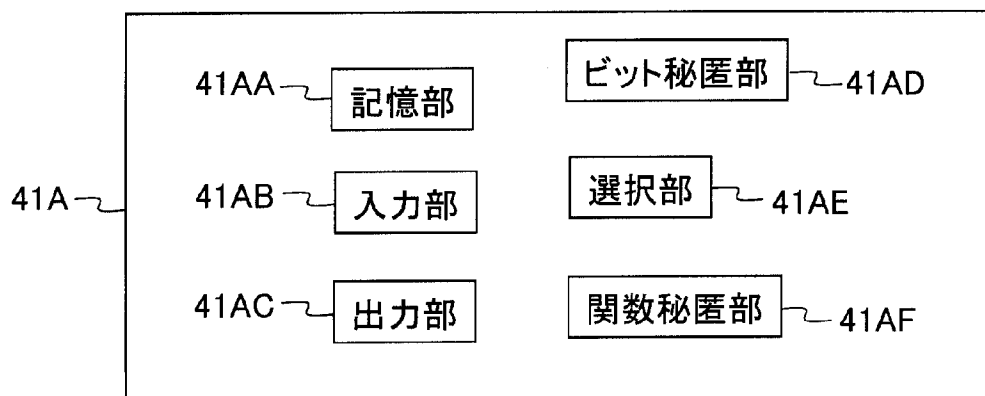


図13

[図14]

(A)



(B)

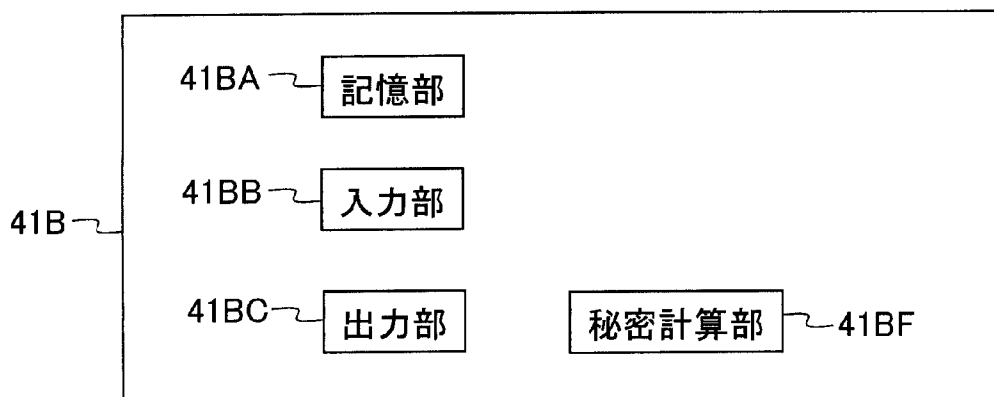


図14

[図15]

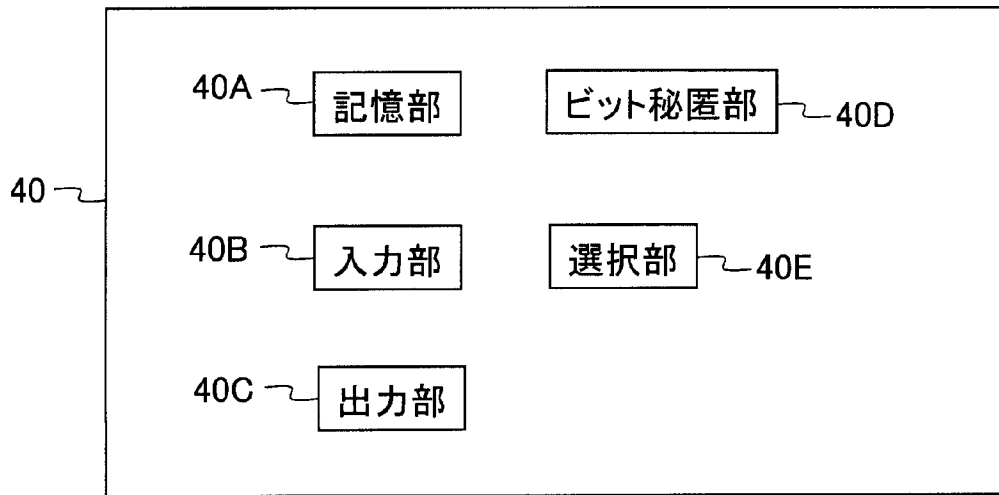


図15

[図16]

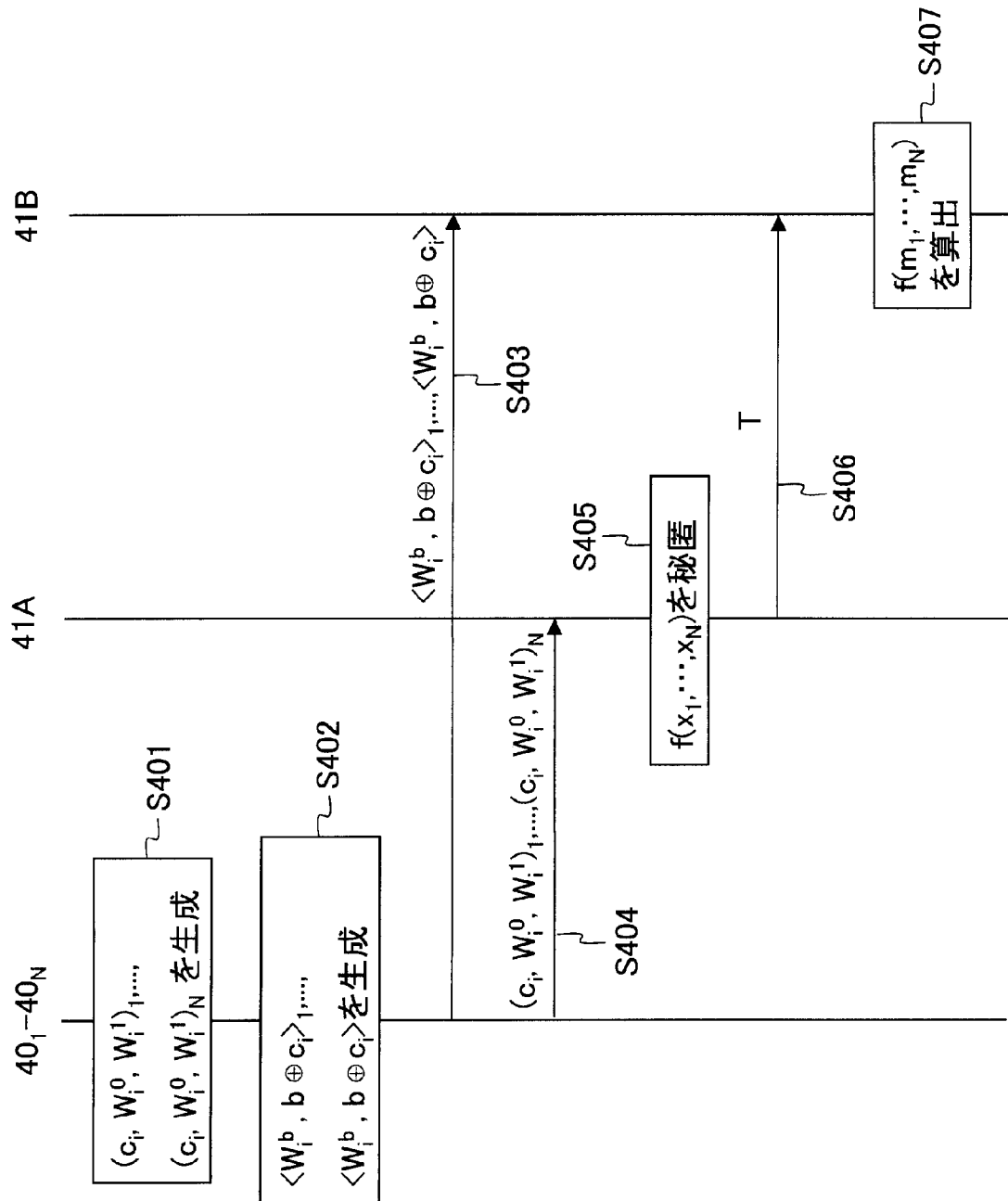


図16

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/050857

A. CLASSIFICATION OF SUBJECT MATTER

G09C1/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2009

Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

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

JSTPlus (JDreamII), JMEDPlus (JDreamII), JST7580 (JDreamII)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Urara SHINMYO, Minoru KURIBAYASHI, Masakatsu MORII, Hatsukazu TANAKA, "Bunsan Server ni Motozuku Oblivious Transfer o Mochiita Denshi Shimon Gijutsu", Proceedings of the 28th Symposium on Information Theory and Its Applications, 20 November, 2005 (20.11.05), Volume II of II, pages 705 to 708	1-25
A	Claude Crepeau, Jeroen van de Graaf, Alain Tapp, "Committed Oblivious Transfer and Private Multi-Party Computation", Lecture Notes in Computer Science, 1995.10.16 (received date), Vol.963, p.110-123, Advances in Cryptology - CRYPTO'95	1-25

☒ 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
13 April, 2009 (13.04.09)Date of mailing of the international search report
21 April, 2009 (21.04.09)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/050857

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Hosseini Ghodosi, Rahim Zaare-Nahandi, "Comments on the 'm out of n oblivious transfer'", Information Processing Letters, 2006.02.28, Volume 97, Number 4, p.153-155	1-25
E,A	Koji Chida and Katsumi Takahashi, "Privacy Preserving Computations without Public Key Cryptographic Operation", LNCS, 2009.02.24 (received date), Vol.5312, p.184-200, Advances in Information and Computer Security	1-25

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

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

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 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JSTPlus(JDreamII), JMEDPlus(JDreamII), JST7580(JDreamII)

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	新名麗, 栗林稔, 森井昌克, 田中初一, “分散サーバに基づく oblivious transfer を用いた電子指紋技術”, 第 28 回情報理論とその応用シンポジウム予稿集, 2005.11.20, V o l u m e II o f II, p. 7 0 5 - 7 0 8	1 - 2 5
A	Claude Crepeau, Jeroen van de Graaf, Alain Tapp, “Committed Oblivious Transfer and Private Multi-Party Computation”, Lecture Notes in Computer Science, 1995.10.16 (受入日), Vol.963, p.110-123, Advances in Cryptology - CRYPTO'95	1 - 2 5

☒ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の 1 以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

1 3 . 0 4 . 2 0 0 9

国際調査報告の発送日

2 1 . 0 4 . 2 0 0 9

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	Hossein Ghodosi, Rahim Zaare-Nahandi, “Comments on the ‘m out of n oblivious transfer’”, Information Processing Letters, 2006.02.28, Volume 97, Number 4, p.153-155	1 – 2 5
E, A	Koji Chida and Katsumi Takahashi, “Privacy Preserving Computations without Public Key Cryptographic Operation”, LNCS, 2009.02.24 (受入日) , Vol.5312, p.184-200, Advances in Information and Computer Security	1 – 2 5