(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
2023年11月16日(16.11.2023)

WIPO | PCT

(10) 国際公開番号
WO 2023/218514 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号： PCT/JP2022/019759

(22) 国際出願日： 2022年5月10日(10.05.2022)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 菅 友梨香 (**SUGA, Yurika**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 山下高生 (**YAMASHITA, Takao**); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP).

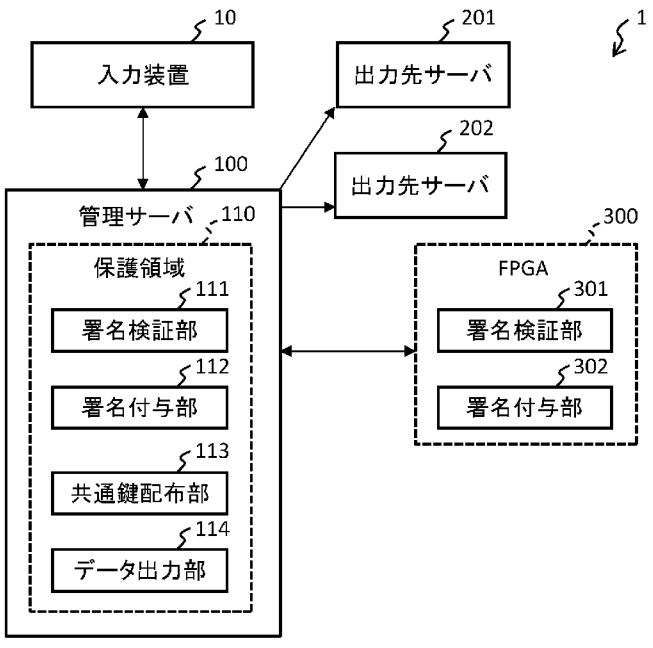
(74) 代理人: 特許業務法人磯野国際特許商標事務所 (**ISONO INTERNATIONAL PATENT OFFICE, P.C.**); 〒1050001 東京都港区虎ノ門一丁目１番１８号 ヒューリック虎ノ門ビル Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH,

(54) **Title:** CALCULATION RESULT DISTRIBUTION DEVICE, CALCULATION RESULT PROTECTION SYSTEM, AND CALCULATION RESULT DISTRIBUTION METHOD

(54) 発明の名称： 計算結果配布装置、計算結果保護システム、および、計算結果配布方法

[図1]



10 Input device
100 Management server
110 Protected area
111, 301 Signature verification unit
112, 302 Signing unit
113 Shared key distribution unit
114 Data output unit
201, 202 Output destination server

(57) **Abstract:** A management server (100) includes: a shared key distribution unit (113) that generates a shared key to be shared among a plurality of output destination servers (201), generates, for each output destination server (201), first encrypted data in which the shared key is encrypted using a public key that is paired with a private key held individually by each output destination server (201), and distributes the generated first encryption data to each output destination server

WO 2023/218514 A1

[続葉有]

KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一　国際調査報告（条約第21条(3)）

(201), thereby allowing each output destination server (201) to decrypt the shared key; and a data output unit (114) that distributes, to each output destination server (201), second encrypted data in which an output value is encrypted using the shared key, thereby allowing each output destination server (201) to decrypt the output value.

(57) 要約：管理サーバ（１００）は、複数の出力先サーバ（２０１）で共用される共通鍵を生成し、各出力先サーバ（２０１）が個別に有する秘密鍵とペアになる公開鍵を用いて、共通鍵を暗号化した第１暗号化データを出力先サーバ（２０１）ごとに生成し、生成した第１暗号化データを出力先サーバ（２０１）ごとに配布することで、各出力先サーバ（２０１）に共通鍵を復号させる共通鍵配布部（１１３）と、共通鍵を用いて出力値が暗号化された第２暗号化データを出力先サーバ（２０１）ごとに配布することで、各出力先サーバ（２０１）に出力値を復号させるデータ出力部（１１４）とを有する。

明　細　書

発明の名称 ：

計算結果配布装置、計算結果保護システム、および、計算結果配布方法

技術分野

[0001] 本発明は、計算結果配布装置、計算結果保護システム、および、計算結果配布方法に関する。

背景技術

[0002] FPGA（field-programmable gate array）は、集積回路の高速性と、処理内容を書き換えられる柔軟性を併せ持つデバイスとして、特定の処理向けに用いられる。クラウドを介してFPGAを利用できるサービスは、FaaS（FPGA as a Service）として知られている。

FaaSでは、例えば、入力装置からの入力値に対して出力値を計算する処理が、クラウドサーバなどの管理サーバからクラウド上のFPGAにオフロードされる。FPGAは、入力値に対して出力値を計算し、その計算した出力値を管理サーバに送る。

[0003] 出力値はクラウドのネットワーク上を流れるので、改ざんなどのセキュリティリスクがあり、情報内容を保護する必要がある。そこで、非特許文献１には、FaaSの環境でセキュリティを高めるためのアーキテクチャとして、共通鍵の生成処理および署名の検証処理をFPGAで行うことが記載されている。

[0004] 図１７は、出力値D2の配布処理を示す説明図である。

まず、第三者機関であるCA（Certificate Authority）は、サービス利用者が使用する入力装置１０ｚと、サービス提供者が使用するＦＰＧＡ３００ｚが生成した公開鍵・秘密鍵ペアの公開鍵を含む証明書を両者に発行する。発行された両者は、それぞれのもつ証明書・秘密鍵を用いて両者で共用される共通鍵CKを事前に生成する。

次に、ＦＰＧＡ３００ｚは、計算した出力値D2に対して共通鍵CKを用いて暗号化した暗号化データCK(D2)を、管理サーバ１００ｚを介して入力装置１

０ｚに送信する。入力装置１０ｚは、受信した暗号化データCK(D2)に対して共通鍵CKを用いて復号することで、安全に出力値D2を得られる。

先行技術文献

非特許文献

[0005] 非特許文献1：Kim, Han-Yee et al. “SafeDB: Spark Acceleration on FPGA Clouds with Enclaved Data Processing and Bitstream Protection.” 2019 IEEE 12th International Conference on Cloud Computing (CLOUD) (2019): 107-114.

発明の概要

発明が解決しようとする課題

[0006] 図１８は、出力値D2の配布先装置が複数存在するときの説明図である。

図１８では、出力値D2の配布先装置が、図１７の入力装置１０ｚと、新たに追加された出力先サーバ２０１ｚ、２０２ｚとで合計３つの装置である。そのため、ＦＰＧＡ３００ｚは、入力装置１０ｚとで共用される共通鍵CK1に加え、出力先サーバ２０１ｚとで共用される共通鍵CK2と、出力先サーバ２０２ｚとで共用される共通鍵CK3とを個別に用意し、その署名を検証する必要がある。

[0007] ＦＰＧＡ３００ｚは、計算した出力値D2に対して共通鍵CK1を用いて暗号化した暗号化データCK1(D2)を、管理サーバ１００ｚを介して入力装置１０ｚに送信する。以下、本明細書では、暗号化されるデータAと、そのデータAに対して暗号化に用いられる鍵Bとで暗号化した結果を、B(A)のようにかっこ書きで表記する。

同様に、ＦＰＧＡ３００ｚは、出力値D2を共通鍵CK2で暗号化した暗号化データCK2(D2)を出力先サーバ２０１ｚに送信し、出力値D2を共通鍵CK3で暗号化した暗号化データCK3(D2)を出力先サーバ２０２ｚに送信する。

このように、ＦＰＧＡ３００ｚは、共通鍵CK1～CK3を生成したり、共通鍵CK1～CK3の署名を検証したり、共通鍵CK1～CK3で暗号化したりする処理を配布

先装置ごとに個別に行う必要がある。その処理負担がＦＰＧＡ３００ｚにかかってしまうため、ＦＰＧＡ３００ｚに出力値D2の計算処理をオフロードする場合でも、処理効率が落ちてしまっていた。

[0008] そこで、本発明は、複数の宛先に同じ計算結果を信頼性ある手法で送信する場合の負担を少なくすることを主な課題とする。

課題を解決するための手段

[0009] 前記課題を解決するために、本発明の計算結果配布装置は、以下の特徴を有する。

本発明は、複数の配布先装置で共用される共通鍵を生成し、

各前記配布先装置が個別に有する秘密鍵とペアになる公開鍵を用いて、前記共通鍵を暗号化した第１暗号化データを前記配布先装置ごとに生成し、生成した前記第１暗号化データを前記配布先装置ごとに配布することで、各前記配布先装置に前記共通鍵を復号させる共通鍵配布部と、

前記共通鍵を用いて計算結果が暗号化された第２暗号化データを前記配布先装置ごとに配布することで、各前記配布先装置に前記計算結果を復号させるデータ出力部とを有することを特徴とする。

発明の効果

[0010] 本発明によれば、複数の宛先に同じ計算結果を信頼性ある手法で送信する場合の負担を少なくすることができる。

図面の簡単な説明

[0011] [図1]本実施形態に関する計算結果保護システムの構成図である。

[図2]本実施形態に関する入力値および出力値の処理を示す説明図である。

[図3]本実施形態に関する共通鍵配布部による共通鍵の配布処理を示す説明図である。

[図4]本実施形態に関するデータ出力部による出力値の配布処理を示す説明図である。

[図5]本実施形態に関する計算結果保護システムの変形例として、出力値の配布先装置に保護領域を設ける場合の構成図である。

[図6]本実施形態に関する図５の場合における共通鍵の配布処理を示す説明図である。

[図7]本実施形態に関する図５の場合における出力値の配布処理を示す説明図である。

[図8]本実施形態に関する出力値の配布先装置が信頼できる相手であることを事前に確認する処理を示すシーケンス図である。

[図9]本実施形態に関する共通鍵の配布処理を示すシーケンス図である。

[図10]本実施形態に関する出力値の配布処理を示すシーケンス図である。

[図11]本実施形態に関する第三者機関としてのＣＡが発行する証明書のリストを示すテーブルである。

[図12]本実施形態に関する管理サーバが有する信頼性がある通信相手のリストを示すテーブルである。

[図13]本実施形態に関する入力装置などの管理サーバ以外の各装置が有する通信相手のリストを示すテーブルである。

[図14]本実施形態に関する管理サーバが有する出力値の配布先装置のリストを示すテーブルである。

[図15]本実施形態に関する管理サーバが有する共通鍵のリストを示すテーブルである。

[図16]本実施形態に関する計算結果保護システムの各装置のハードウェア構成図である。

[図17]出力値の配布処理を示す説明図である。

[図18]出力値の配布先装置が複数存在するときの説明図である。

[図19]本実施形態に関する図４の変形例として、管理サーバの代わりにＦＰＧＡが暗号化処理を実行するときの説明図である。

発明を実施するための形態

[0012] 以下、本発明の一実施形態について、図面を参照して詳細に説明する。

[0013] 図１は、計算結果保護システム１の構成図である。

計算結果保護システム１は、入力装置１０と、管理サーバ（計算結果配布

装置）１００と、ＦＰＧＡ（オフロード先装置）３００と、出力先サーバ２０１と、出力先サーバ２０２とがネットワークで接続されて構成される。

入力装置１０は、ＦＰＧＡ３００にオフロードする処理として、入力値D1から出力値D2（計算結果）を計算する処理（以下、オフロード処理）を管理サーバ１００に依頼する。つまり、入力装置１０は、入力値D1を管理サーバ１００に送信する。

[0014] なお、オフロード先装置は、ＦＰＧＡ３００に限定されず、以下に例示されるような任意のデバイスを用いてもよい。

・GPU (Graphics Processing Unit)

・FPU (Floating Point Unit)

・DSP (Digital Signal Processor)

[0015] 管理サーバ１００は、入力装置１０から受け付けたオフロード処理を、ＦＰＧＡ３００にオフロードする。ＦＰＧＡ３００は、受け付けたオフロード処理を実行することで得た出力値D2を、管理サーバ１００に返信する。管理サーバ１００は、ＦＰＧＡ３００から得た出力値D2を、配布先装置に配布する。配布先装置とは、図１では、入力装置１０と、出力先サーバ２０１と、出力先サーバ２０２とで合計３台の装置である。また、管理サーバ１００は、配布先装置の詳細な状態を確認する。

[0016] なお、オフロード処理は、例えば、セキュリティを検証する装置の情報を入力値D1とし、その入力値D1からセキュリティの信頼性スコアなどの出力値D2を計算する処理である。つまり、入力値D1も出力値D2も、データ内容が改ざんされていないなどの信頼性が求められる重要な情報であるため、その計算を誰が行ったのかという計算主体を示す署名も併せて用意する必要がある。

そのため、管理サーバ１００内のメモリには、保護領域（第１保護領域）１１０が用意される。

[0017] 保護領域１１０は、不正なデータアクセスから格納されるデータを保護する。つまり、保護領域１１０とは、管理サーバ１００のメモリ内に用意されるデータアクセス権限が保護された領域（enclave）であり、アクセス権限を

一部のアプリケーションに絞ることで、データを保護できる。

保護領域１１０は、強い権限を持ったソフトウェアが攻撃された場合に、弱い権限を持ったソフトウェアまで侵害されるのを防ぐ目的で用意される。強い権限を持ったソフトウェアとは、例えば、OS（Operating System）、ドライバ、BIOS（Basic Input Output System）、VMM（Virtual Machine Manager）である。

[0018] なお、管理サーバ１００は、情報を保護しながら署名や暗号化などのプログラムを実行できる保護領域１１０を構成する。保護領域１１０は、例えば、署名・署名検証のプログラムの追加で完全性を確保できる場所である。さらに、保護領域１１０は、アクセス権限が限られている隔離された場所であり、暗号化のプログラムを追加することで機密性も確保できる。

保護領域１１０は、内部のすべてのデータが安全に守られている場合が望ましいが、完全に守られていなくても、内部のデータのうちの秘密の情報（公開鍵暗号技術における秘密鍵など）が安全に守られている場合も利用可能とする。

[0019] 具体的には、管理サーバ１００の保護領域１１０には、署名検証部１１１と、署名付与部１１２と、共通鍵配布部１１３と、データ出力部１１４とが構成されており、これらの各処理部の処理に用いられるデータが、保護領域１１０内に格納される。

署名検証部１１１は、例えば、他装置から送付された他装置の機器情報を参照して、他装置が保護領域（データの保護能力）を有している場合に、検証に合格と判定する。検証に合格した配布先装置は、出力値D2の配布対象となる。これにより、管理サーバ１００から他装置に送付された情報が、他装置内の保護領域に格納されることが保証されるので、配布先装置の他装置からの情報流出を配布前に抑制できる。

他装置の機器情報は、例えば、他装置の保護領域のアドレス情報や、保護領域内のアプリケーションの情報など、保護領域などの能力を確認する技術であるアテステーションに用いられる情報である。

[0020] 署名検証部１１１は、管理サーバ１００にとって通信相手となる他装置（入力装置１０など）の署名を検証することで、他装置の信頼性を確認してもよい。そのため、署名検証部１１１は、以下に例示する情報のうちの少なくとも１つになされた署名を検証する。

・第三者機関（CA）が発行する証明書。または、その証明書に含まれる他装置の公開鍵。

・他装置から発行された乱数情報。

・他装置のアドレス情報（IPアドレスなど）。

・他装置の公開鍵に紐づいた他装置の機器情報。

[0021] 署名付与部１１２は、管理サーバ１００自身の信頼性を他装置に確認させるための署名を付与する。なお、どのような情報に対して署名を付与するかについては、署名検証部１１１が検証した他装置の各情報を、管理サーバ１００の各情報に置き換えたものを用いればよい。

共通鍵配布部１１３は、ＦＰＧＡ３００の出力値（計算結果）を暗号化するときに用いられる複数の通信相手に共用される共通鍵を生成し、その共通鍵を他装置に配布する。

[0022] つまり、共通鍵配布部１１３は、複数の配布先装置（入力装置１０など）で共用される共通鍵CKを生成する。そして、共通鍵配布部１１３は、各配布先装置が個別に有する秘密鍵SKとペアになる公開鍵PKを用いて、共通鍵CKを暗号化した第１暗号化データを配布先装置ごとに生成する。さらに、共通鍵配布部１１３は、生成した第１暗号化データを配布先装置ごとに配布することで、各配布先装置に共通鍵CKを復号させる。

[0023] データ出力部１１４は、共通鍵配布部１１３が生成した共通鍵CKを用いて、ＦＰＧＡ３００の出力値D2（計算結果）を暗号化した第２暗号化データを生成する（詳細は図４）。そして、データ出力部１１４は、生成した第２暗号化データを配布先装置ごとに配布することで、各配布先装置に出力値D2を復号させる。

または、共通鍵配布部１１３が生成した共通鍵CKをＦＰＧＡ３００に送り

、ＦＰＧＡ３００上で出力値D2を暗号化した第２暗号化データを生成してもよい（詳細は図１９）。

[0024] ＦＰＧＡ３００は、署名検証部３０１と、署名付与部３０２とを有する。

署名検証部３０１は、オフロード元である管理サーバ１００の署名付与部１１２が付与した署名を検証することで、管理サーバ１００を検証する。

署名付与部３０２は、ＦＰＧＡ３００自身の信頼性を他装置に確認させるための署名を、ＦＰＧＡ３００の出力値に付与する。

[0025] 図２は、入力値D1および出力値D2の処理を示す説明図である。

入力装置１０は、用意した入力値D1に対して、自身の鍵s10を用いて署名s10(D1)を作成する。入力装置１０は、入力値D1と署名s10(D1)とを管理サーバ１００の保護領域１１０に送付する。

保護領域１１０の署名検証部１１１は、署名s10(D1)を検証する。署名付与部１１２は、署名検証部１１１の検証に合格した署名s10(D1)に対して、自身の鍵s100を用いた署名s100(D1)に置き換える。署名付与部１１２は、署名s100(D1)とともに入力値D1のオフロード処理をＦＰＧＡ３００に依頼する。

[0026] ＦＰＧＡ３００の署名検証部３０１は、依頼されたオフロード処理の署名s100(D1)を検証する。ＦＰＧＡ３００は、署名検証部３０１の検証に合格した署名s100(D1)の入力値D1をもとに、オフロード処理を計算することで出力値D2を得る。

署名付与部３０２は、計算した出力値D2に対して、自身の鍵s300を用いて署名s300(D2)を作成する。ＦＰＧＡ３００は、出力値D2とその署名s300(D2)とを、管理サーバ１００の保護領域１１０に送付する。

署名検証部１１１は、受信した出力値D2とその署名s300(D2)とを検証する。署名付与部１１２は、検証に合格した署名s300(D2)を署名SK100(D2)に置き換える。

データ出力部１１４は、配布先装置である入力装置１０と、出力先サーバ２０１と、出力先サーバ２０２とに出力値D2と署名SK100(D2)とを配布する。

[0027] 図３は、共通鍵配布部１１３による共通鍵CKの配布処理を示す説明図であ

る。

共通鍵配布部１１３は、図２で示した出力値D2の配布処理に伴う暗号化を行うために、複数の配布先装置で共用する共通鍵CKを以下の手順で配布する。

（手順１）　共通鍵配布部１１３は、配布先装置ごとに検証済みの公開鍵PKとして、入力装置１０の公開鍵PK10と、出力先サーバ２０１の公開鍵PK201と、出力先サーバ２０２の公開鍵PK202とをCAや配布先装置などから事前に取得しておく。

（手順２）　共通鍵配布部１１３は、複数の配布先装置で共用する共通鍵CKを１つ生成する。

（手順３）　共通鍵配布部１１３は、配布先装置ごとの公開鍵PKで共通鍵CKを暗号化した暗号化データを複数生成する。例えば、入力装置１０向けの暗号化データPK10(CK)は、入力装置１０の公開鍵PK10で共通鍵CKを暗号化したものである。

[0028] （手順４）　共通鍵配布部１１３は、生成した複数の暗号化データを、それぞれの配布先装置に配布する。例えば、暗号化データPK10(CK)は入力装置１０に配布され、暗号化データPK201(CK)は出力先サーバ２０１に配布され、暗号化データPK202(CK)は出力先サーバ２０２に配布される。

（手順５）　各配布先装置は、手順１の公開鍵PKとペアになる自身の秘密鍵SKを用いて、配布された暗号化データを復号することで、手順２の共通鍵CKを取得する。例えば、入力装置１０は、自身の秘密鍵SK10を用いて、配布された暗号化データPK10(CK)を復号することで、手順２の共通鍵CKを取得する。

以上の手順により、管理サーバ１００が生成した１つの共通鍵CKが、保護領域１１０から各配布先装置に安全に配布された。管理サーバ１００は、配布先装置の台数に関係なく共通鍵CKを１つ生成すればよいので、負荷が下がる。

[0029] 図４は、データ出力部１１４による出力値D2の配布処理を示す説明図であ

る。

データ出力部１１４は、以下の手順により図３で示した共通鍵CKを用いて出力値D2の暗号化を行ってから配布することで、出力値D2の安全性を確保できる。

（手順１）　データ出力部１１４は、オフロード先のＦＰＧＡ３００から受信した出力値D2と、その署名s300(D2)とを受信する。以下、受信した出力値D2と、その署名s300(D2)とをつなげた全体のデータを「D2||s300(D2)」のように、記号「||」で示す。

（手順２）　データ出力部１１４は、共通鍵CKを用いてデータD2||s300(D2)の暗号化を行うことで、暗号化データCK(D2||s300(D2))を取得する。

（手順３）　データ出力部１１４は、暗号化データCK(D2||s300(D2))を各配布先装置に配布する。

（手順４）　入力装置１０などの各配布先装置は、共通鍵CKを用いて暗号化データCK(D2||s300(D2))からデータD2||s300(D2)を復号する。また各配布先装置は、出力値D2と、その署名s300(D2)とを検証する。

このように、データ出力部１１４は、配布先装置が複数であっても、配布した共通鍵CKを用いた暗号化を一度行えばよい。よって、配布先装置が増えても、暗号化の手間が増えずに済む。

[0030]　図１９は、図４の変形例として、管理サーバ１００の代わりに、ＦＰＧＡ３００が暗号化するときの説明図である。図４の（手順１）、（手順２）が、以下の（手順１Ｂ）、（手順２Ｂ）に置き換わる。（手順２Ｂ）の後は図４と同様に、（手順３）、（手順４）が実行される。

（手順１Ｂ）　ＦＰＧＡ３００は、管理サーバ１００から受信した共通鍵CKを用いてデータD2||s300(D2)の暗号化を行うことで、暗号化データCK(D2||s300(D2))を取得する。

（手順２Ｂ）　データ出力部１１４は、オフロード先のＦＰＧＡ３００から暗号化データCK(D2||s300(D2))を受信する。

[0031]　図５は、計算結果保護システム１の変形例として、出力値D2の配布先装置

に保護領域（第２保護領域）を設ける場合の構成図である。

図１の計算結果保護システム１と比較すると、出力値D2の配布先装置である各装置（入力装置１０と、出力先サーバ２０１と、出力先サーバ２０２と）は、それぞれ自身に保護領域１０ｐ、２０１ｐ、２０２ｐを有している。

図６は、図５の場合における共通鍵CKの配布処理を示す説明図である。図５では図３の（手順５）で共通鍵CKを復号する処理が、各装置の保護領域内で行うように変更されている。

図７は、図５の場合における出力値D2の配布処理を示す説明図である。図５では図４の（手順４）で暗号化データCK(D2||s300(D2))を復号する処理が、各装置の保護領域内で行うように変更されている。

以上、図５～図７の構成により、出力値D2が外部から不正アクセスされずに済み、セキュリティ強度が向上する。以下、図８～図１６を参照して、図２～図４の処理の詳細を説明する。

[0032] 図８は、出力値D2の配布先装置が信頼できる相手であることを事前に確認する処理を示すシーケンス図である。

このシーケンス図では、計算結果保護システム１の各装置が、チャレンジ／レスポンス認証（challenge and response authentication）により、パスワードなどの秘密の情報を直接やり取りすることなく、他装置を確認する。

[0033] まず、Ｓ１０１－Ｓ１０４により管理サーバ１００が入力装置１０の公開鍵PK10を確認する。

具体的には、管理サーバ１００は、乱数R1を入力装置１０に送付する（Ｓ１０１）。入力装置１０は、乱数R1に自身の秘密鍵SK10を用いて、署名SK10(R1)を生成する（Ｓ１０２）。

入力装置１０は、自身の公開鍵PK10および署名SK10(R1)を管理サーバ１００に送付する（Ｓ１０３）。管理サーバ１００の署名検証部１１１は、送付された公開鍵PK10を署名SK10(R1)で確認する（Ｓ１０４）。Ｓ１０４の確認に成功した場合、次のＳ１１１に処理を進める。

一方、Ｓ１０４の確認に失敗した場合、エラーメッセージを通信相手の入

力装置１０に返信する。以降の各処理においても、署名の確認に失敗した場合、エラーメッセージを通信相手に返信する。

[0034] 図１１は、第三者機関としてのCAが発行する証明書のリストを示すテーブルである。

このテーブルには、証明書IDと、証明書に含まれる公開鍵と、その公開鍵とペアになる秘密鍵と、秘密鍵を管理する主体者と、証明書を発行するCAである発行者と、証明書の有効期限とが対応付けられている。計算結果保護システム１の各装置（例えば管理サーバ１００）は、CAから証明書により有効期限内で信頼性が保障された公開鍵（例えば入力装置１０の公開鍵PK10）を取得できる。

証明書は、PKI（Public Key Infrastructure）という環境で利用される。PKIでは、RSA暗号や楕円曲線暗号などの各種の暗号化技術を利用して、第三者機関(CA)による証明書発行先の保証をもとにした、通信相手の認証やAttestationを行うことができる。

各装置は、自身の証明書およびその証明書に付属する秘密鍵＆公開鍵のペアを、事前にCAから入手しておく。あるいは、各装置で、公開鍵＆秘密鍵のペアを作成して、その公開鍵を使った証明書を事前にCAから入手しておく。一方、他装置の公開鍵は、CAから入手するのではなく、他装置に送付してもらう。

[0035] 図１２は、管理サーバ１００が有する信頼性がある通信相手のリストを示すテーブルである。

このテーブルには、図１１で説明した各項目（証明書IDと、公開鍵と、主体者と、発行者と、有効期限）に加え、主体者の装置のIPアドレスが公開鍵に紐づいた機器情報として対応付けられている。つまり、他装置の主体者の列を検索キーとして、他装置の機器情報や、他装置の保護領域のアドレス（図示省略）、保護領域内のアプリケーションの情報（図示省略）なども、Ｓ１１４の処理や後記するＳ１３４の処理で確認できる。

また、このテーブルには、Ｓ１０１－Ｓ１０４で確認された入力装置１０

のエントリに加え、後記するＳ１２０で通知された出力先サーバ２０１，２０２のエントリも含まれる。なお、図１２のテーブルの状態は、以下で説明するＳ１３１－Ｓ１３４により出力先サーバ２０１，２０２が確認された後の状態である。

[0036] 図８に戻り、Ｓ１１１－Ｓ１１４により入力装置１０が管理サーバ１００の公開鍵PK100を確認する。

具体的には、入力装置１０は、乱数R2を管理サーバ１００に送付する（Ｓ１１１）。管理サーバ１００の署名付与部１１２は、乱数R2に自身の秘密鍵SK100を用いて、署名SK100(R2)を生成する（Ｓ１１２）。

管理サーバ１００は、自身の公開鍵PK100および署名SK100(R2)を入力装置１０に送付する（Ｓ１１３）。入力装置１０は、送付された公開鍵PK100を署名SK100(R2)で確認する（Ｓ１１４）。

入力装置１０は、これから確認が必要な出力先サーバ２０１，２０２の情報を管理サーバ１００に送付する（Ｓ１２０）。

[0037] 図１３は、入力装置１０などの管理サーバ１００以外の各装置が有する通信相手のリストを示すテーブルである。このテーブルは図１２と同じデータ形式である。図１２と同様に、図１３のテーブルには、Ｓ１１１－Ｓ１１４の結果として、入力装置１０にとって、信頼できる相手である管理サーバ１００のエントリが登録される。

[0038] 図８に戻り、Ｓ１３１－Ｓ１３４により管理サーバ１００が出力先サーバ２０１の公開鍵PK201を確認する。なお、図示は省略するが、管理サーバ１００が出力先サーバ２０２の公開鍵PK202を確認する処理も同様である。

管理サーバ１００は、乱数R3を出力先サーバ２０１に送付する（Ｓ１３１）。出力先サーバ２０１は、乱数R3に自身の秘密鍵SK201を用いて、署名SK201(R3)生成する（Ｓ１３２）。

出力先サーバ２０１は、自身の公開鍵PK201および署名SK201(R3)を管理サーバ１００に送付する（Ｓ１３３）。管理サーバ１００の署名検証部１１１は、送付された公開鍵PK201を署名SK201(R3)で確認する（Ｓ１３４）。

[0039] 図１４は、管理サーバ１００が有する出力値D2の配布先装置のリストを示すテーブルである。このテーブルは、同じ出力値D2の配布先装置ごとに発行される要求IDと、同じ出力値D2の配布先装置を示す送付先と、その送付先に対して発行される図１１の情報（証明書のIDと、その送付先の公開鍵）と、図１２のIPアドレスとが対応付けられている。

例えば、要求IDが同じ「R01」である３つの装置（入力装置１０、出力先サーバ２０１、出力先サーバ２０２）が、同じ出力値D2の配布先装置となる集合である。管理サーバ１００は、図８の処理で確認された装置を、図１４のテーブルに順次追加する。

[0040] 図１５は、管理サーバ１００が有する共通鍵CKのリストを示すテーブルである。このテーブルには、図１４の要求IDごとに発行された共通鍵CKが登録される。

もし、出力値D2の配布先装置とは別に、出力値D3を２つの装置（入力装置１０、出力先サーバ２０１）に配布したい場合、管理サーバ１００は、新たな要求ID「R02」と、その配布先装置と、そのR02用に発行された新たな共通鍵CK2との組み合わせを、図１４のテーブルおよび図１５のテーブルに追加すればよい。

[0041] 図９は、共通鍵CKの配布処理を示すシーケンス図である。

管理サーバ１００は、複数の配布先装置で共用する共通鍵CKを作成する（Ｓ２０１）。管理サーバ１００は、図８で確認した入力装置１０の公開鍵PK10を用いて、共通鍵CKを暗号化した暗号化データPK10(CK)を作成する（Ｓ２０２）。管理サーバ１００は、暗号化データPK10(CK)を入力装置１０に送付する（Ｓ２０３）。

入力装置１０は、自身の秘密鍵SK10で暗号化データPK10(CK)を復号することで、共通鍵CKを取得する（Ｓ２０４）。

[0042] 以上は、入力装置１０を配布先装置とした場合の処理であるが、Ｓ２０２－Ｓ２０４は、出力値D2の配布先装置ごとに実行される。以下に示すように、他の配布先装置も同様に図９の処理を実行する。

［Ｓ２０３の配布先装置＝出力先サーバ２０１の場合］　Ｓ２０２で暗号化データの作成に用いられる公開鍵PK10が、図８で確認した出力先サーバ２０１の公開鍵PK201に置き換わる。Ｓ２０４で暗号化データの復号に用いられる秘密鍵SK10が、出力先サーバ２０１の秘密鍵SK201に置き換わる。

［Ｓ２０３の配布先装置＝出力先サーバ２０２の場合］　Ｓ２０２で暗号化データの作成に用いられる公開鍵PK10が、図８で確認した出力先サーバ２０２の公開鍵PK202に置き換わる。Ｓ２０４で暗号化データの復号に用いられる秘密鍵SK10が、出力先サーバ２０２の秘密鍵SK202に置き換わる。

[0043] 図１０は、出力値D2の配布処理を示すシーケンス図である。

管理サーバ１００は、出力値D2と、その署名s300(D2)と、その検証用の公開鍵PKsを、オフロード先のＦＰＧＡ３００から取得する（Ｓ３０１）。そのため、ＦＰＧＡ３００には、署名s300(D2)を生成するための秘密鍵SKsと、その検証用の公開鍵PKsとが事前に用意される。

管理サーバ１００は、共通鍵CKを用いてデータD2||s300(D2)の暗号化を行うことで、暗号化データCK(D2||s300(D2))を作成する（Ｓ３０２）。管理サーバ１００は、暗号化データCK(D2||s300(D2))と、公開鍵PKsとを、入力装置１０に送付する（Ｓ３０３）。

[0044] 入力装置１０は、共通鍵CKを用いて暗号化データCK(D2||s300(D2))からデータD2||s300(D2)を復号して取得する（Ｓ３０４）。入力装置１０は、公開鍵PKsで署名s300(D2)を復号して、出力値D2の署名として正当か否かを検証する（Ｓ３０５）。Ｓ３０５の署名の確認に成功した場合には、データの改ざんがなされていないことを確認できる。

以上は、入力装置１０を配布先装置とした場合の処理であるが、Ｓ３０３、Ｓ３０４は、出力値D2の配布先装置ごとに（出力先サーバ２０１、出力先サーバ２０２）実行される。

[0045] 図１６は、計算結果保護システム１の各装置のハードウェア構成図である。

計算結果保護システム１の各装置は、ＣＰＵ９０１と、ＲＡＭ９０２と、

ＲＯＭ９０３と、ＨＤＤ９０４と、通信Ｉ／Ｆ９０５と、入出力Ｉ／Ｆ９０６と、メディアＩ／Ｆ９０７と、ＴＰＭ（Trusted Platform Module）９０８とを有するコンピュータ９００として構成される。

通信Ｉ／Ｆ９０５は、外部の通信装置９１５と接続される。入出力Ｉ／Ｆ９０６は、入出力装置９１６と接続される。メディアＩ／Ｆ９０７は、記録媒体９１７からデータを読み書きする。さらに、ＣＰＵ９０１は、ＲＡＭ９０２に読み込んだプログラム（アプリケーションや、その略のアプリとも呼ばれる）を実行することにより、各部を制御する。そして、このプログラムは、通信回線を介して配布したり、ＣＤ－ＲＯＭ等の記録媒体９１７に記録して配布したりすることも可能である。

さらに、ＴＰＭ９０８は、ＲＡＭ９０２内に保護領域を形成するためなどに使用される。

[0046] ［効果］

本発明の管理サーバ１００は、複数の配布先装置（入力装置１０など）で共用される共通鍵CKを生成し、

各配布先装置が個別に有する秘密鍵SKとペアになる公開鍵PKを用いて、共通鍵CKを暗号化した暗号化データPK10(CK)を配布先装置ごとに生成し、生成した暗号化データPK10(CK)を配布先装置ごとに配布することで、各配布先装置に共通鍵CKを復号させる共通鍵配布部１１３と、

共通鍵CKを用いて出力値D2が暗号化された暗号化データCK(D2)を配布先装置ごとに配布することで、各配布先装置に出力値D2を復号させるデータ出力部１１４とを有することを特徴とする。

[0047] これにより、複数の配布先装置にデータを送るときに同じ共通鍵CKを使用するので、管理サーバ１００は、複数の共通鍵CKを生成および保持しなくてもよい。よって、共通鍵CKの統合管理によりセキュリティリソースの管理コストを削減できる。また、出力値D2を計算するＦＰＧＡ３００の処理負担を削減できる。

また、共通鍵CKを用いた暗号化処理や復号処理は、秘密鍵SK・公開鍵PKを

用いた暗号化処理や復号処理よりも負荷が少ないので、頻度の高い出力値D2の暗号化処理や復号処理を低負荷で実行できる。よって、複数の宛先に同じ計算結果を信頼性ある手法で送信する場合の負担を少なくできる。

[0048] 本発明は、管理サーバ１００が、不正なデータアクセスから格納されるデータを保護する保護領域１１０を有しており、

共通鍵配布部１１３の処理に用いられるデータ、および、データ出力部１１４の処理に用いられるデータが、保護領域１１０内に格納されることを特徴とする。

[0049] これにより、共通鍵CKなどの暗号鍵が管理サーバ１００内の保護領域１１０で安全に保管される。

[0050] 本発明は、前記の管理サーバ１００と、配布先装置とを有する計算結果保護システム１であって、

少なくとも一部の配布先装置が、不正なデータアクセスから格納されるデータを保護する保護領域１０ｐを有しており、

管理サーバ１００が、さらに、各配布先装置を保護領域１１０内で検証する署名検証部１１１を有しており、

署名検証部１１１が、配布先装置の機器情報を参照して配布先装置が保護領域１０ｐを有するか否かを検証し、保護領域１０ｐを有する配布先装置を検証に合格とし、その合格した配布先装置に生成した暗号化データPK10(CK)を配布することを特徴とする。

[0051] これにより、秘匿度の高い情報を管理サーバ１００から他装置に送付する場合に、他装置内の保護領域に秘匿度の高い情報が格納されることが事前に保証される。よって、配布先装置の他装置からの情報流出を配布前に抑制できる。

[0052] 本発明は、計算結果保護システム１が、さらに、出力値D2を計算するＦＰＧＡ３００を有しており、

ＦＰＧＡ３００が、計算した出力値D2と、自身の署名とを管理サーバ１００に送付し、

データ出力部１１４が、暗号化データCK(D2)と、ＦＰＧＡ３００の署名とを配布先装置ごとに配布し、

配布先装置が、暗号化データCK(D2)を復号した出力値D2と、ＦＰＧＡ３００の署名とを保護領域１０ｐ内で検証することを特徴とする。

[0053] これにより、出力値D2がＦＰＧＡ３００の計算結果であることを保証でき、出力値D2の改ざんが発生したとしても、適切に改ざんを検出できる。

符号の説明

[0054]

１　計算結果保護システム

１０　入力装置（配布先装置）

１０ｐ　保護領域（第２保護領域）

１００　管理サーバ（計算結果配布装置）

１１０　保護領域（第１保護領域）

１１１　署名検証部（検証部）

１１２　署名付与部

１１３　共通鍵配布部

１１４　データ出力部

２０１　出力先サーバ（配布先装置）

２０１ｐ　保護領域（第２保護領域）

２０２　出力先サーバ（配布先装置）

２０２ｐ　保護領域（第２保護領域）

３００　ＦＰＧＡ（オフロード先装置）

３０１　署名検証部

３０２　署名付与部

請求の範囲

[請求項1] 複数の配布先装置で共用される共通鍵を生成し、

各前記配布先装置が個別に有する秘密鍵とペアになる公開鍵を用いて、前記共通鍵を暗号化した第１暗号化データを前記配布先装置ごとに生成し、生成した前記第１暗号化データを前記配布先装置ごとに配布することで、各前記配布先装置に前記共通鍵を復号させる共通鍵配布部と、

前記共通鍵を用いて計算結果が暗号化された第２暗号化データを前記配布先装置ごとに配布することで、各前記配布先装置に前記計算結果を復号させるデータ出力部とを有することを特徴とする

計算結果配布装置。

[請求項2] 前記計算結果配布装置は、不正なデータアクセスから格納されるデータを保護する第１保護領域を有しており、

前記共通鍵配布部の処理に用いられるデータ、および、前記データ出力部の処理に用いられるデータは、前記第１保護領域内に格納されることを特徴とする

請求項１に記載の計算結果配布装置。

[請求項3] 請求項２に記載の計算結果配布装置と、前記配布先装置とを有する計算結果保護システムであって、

少なくとも一部の前記配布先装置は、不正なデータアクセスから格納されるデータを保護する第２保護領域を有しており、

前記計算結果配布装置は、さらに、各前記配布先装置を前記第１保護領域内で検証する検証部を有しており、

前記検証部は、前記配布先装置の機器情報を参照して前記配布先装置が前記第２保護領域を有するか否かを検証し、前記第２保護領域を有する前記配布先装置を検証に合格とし、その合格した前記配布先装置に生成した前記第１暗号化データを配布することを特徴とする

計算結果保護システム。

[請求項4] 前記計算結果保護システムは、さらに、前記計算結果を計算するオフロード先装置を有しており、

前記オフロード先装置は、計算した前記計算結果と、自身の署名とを前記計算結果配布装置に送付し、

前記データ出力部は、前記第２暗号化データと、前記オフロード先装置の署名とを前記配布先装置ごとに配布し、

前記配布先装置は、前記第２暗号化データを復号した前記計算結果と、前記オフロード先装置の署名とを前記第２保護領域内で検証することを特徴とする

請求項３に記載の計算結果保護システム。

[請求項5] 計算結果配布装置は、共通鍵配布部と、データ出力部とを有しており、

前記共通鍵配布部は、

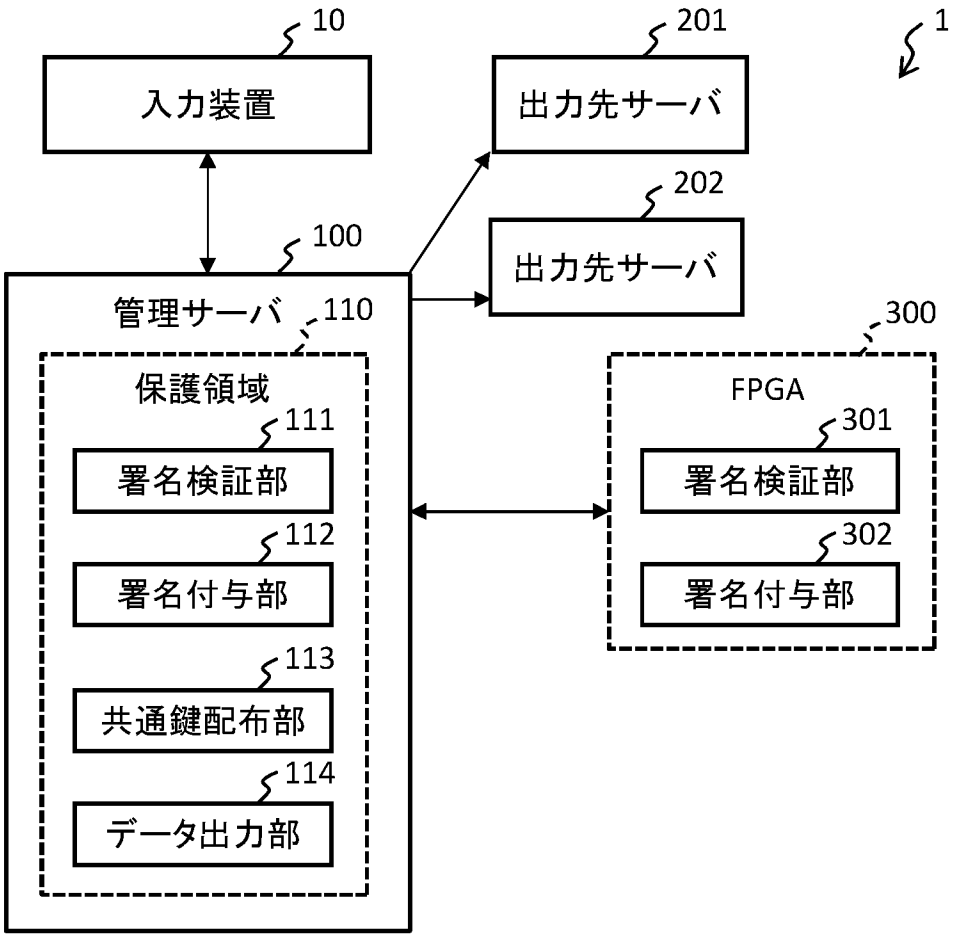
複数の配布先装置で共用される共通鍵を生成し、

各前記配布先装置が個別に有する秘密鍵とペアになる公開鍵を用いて、前記共通鍵を暗号化した第１暗号化データを前記配布先装置ごとに生成し、生成した前記第１暗号化データを前記配布先装置ごとに配布することで、各前記配布先装置に前記共通鍵を復号させ、

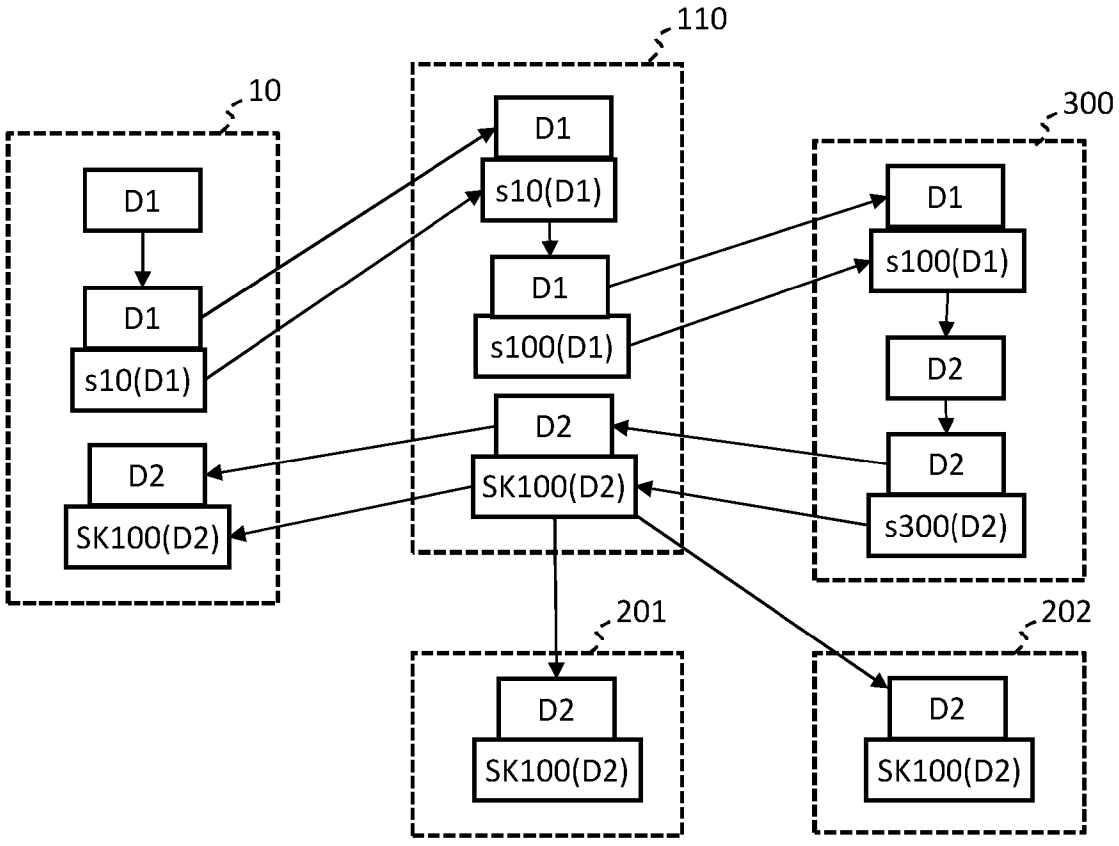
前記データ出力部は、前記共通鍵を用いて計算結果が暗号化された第２暗号化データを前記配布先装置ごとに配布することで、各前記配布先装置に前記計算結果を復号させることを特徴とする

計算結果配布方法。

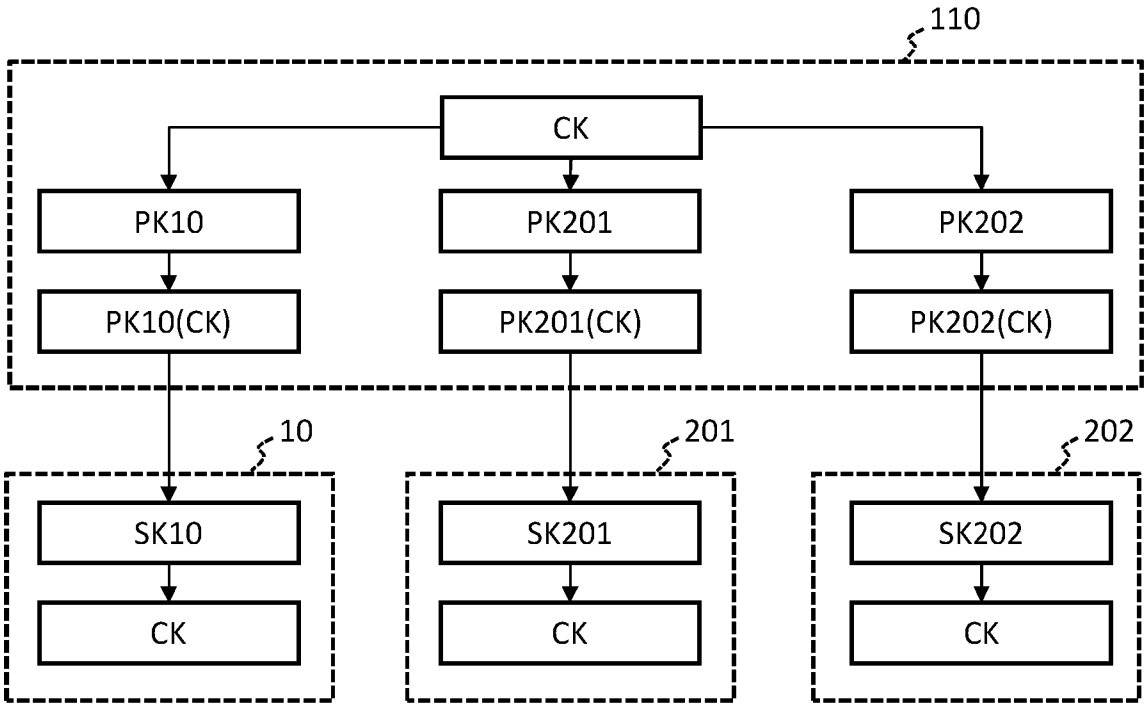
[図1]


10
入力装置
201
出力先サーバ
1
202
出力先サーバ
100
管理サーバ
110
保護領域
111
署名検証部
112
署名付与部
113
共通鍵配布部
114
データ出力部
300
FPGA
301
署名検証部
302
署名付与部

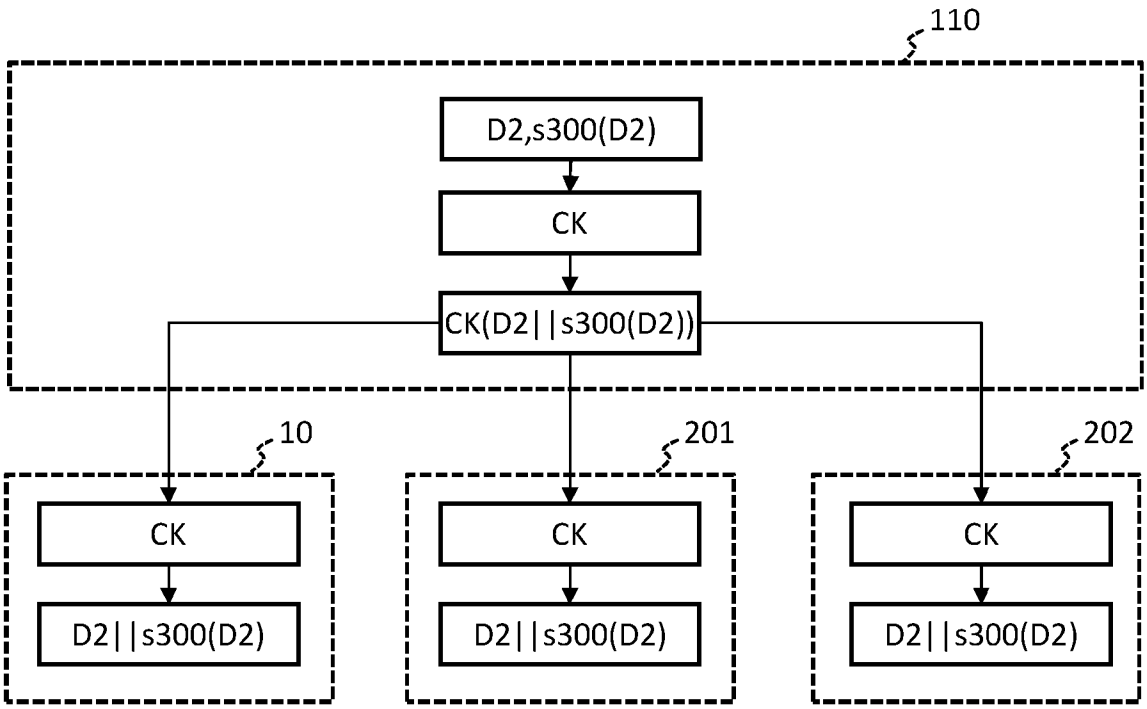
[図2]


110
10
D1
D1
s10(D1)
D2
SK100(D2)
D1
s10(D1)
D1
s100(D1)
D2
SK100(D2)
300
D1
s100(D1)
D2
D2
s300(D2)
201
D2
SK100(D2)
202
D2
SK100(D2)

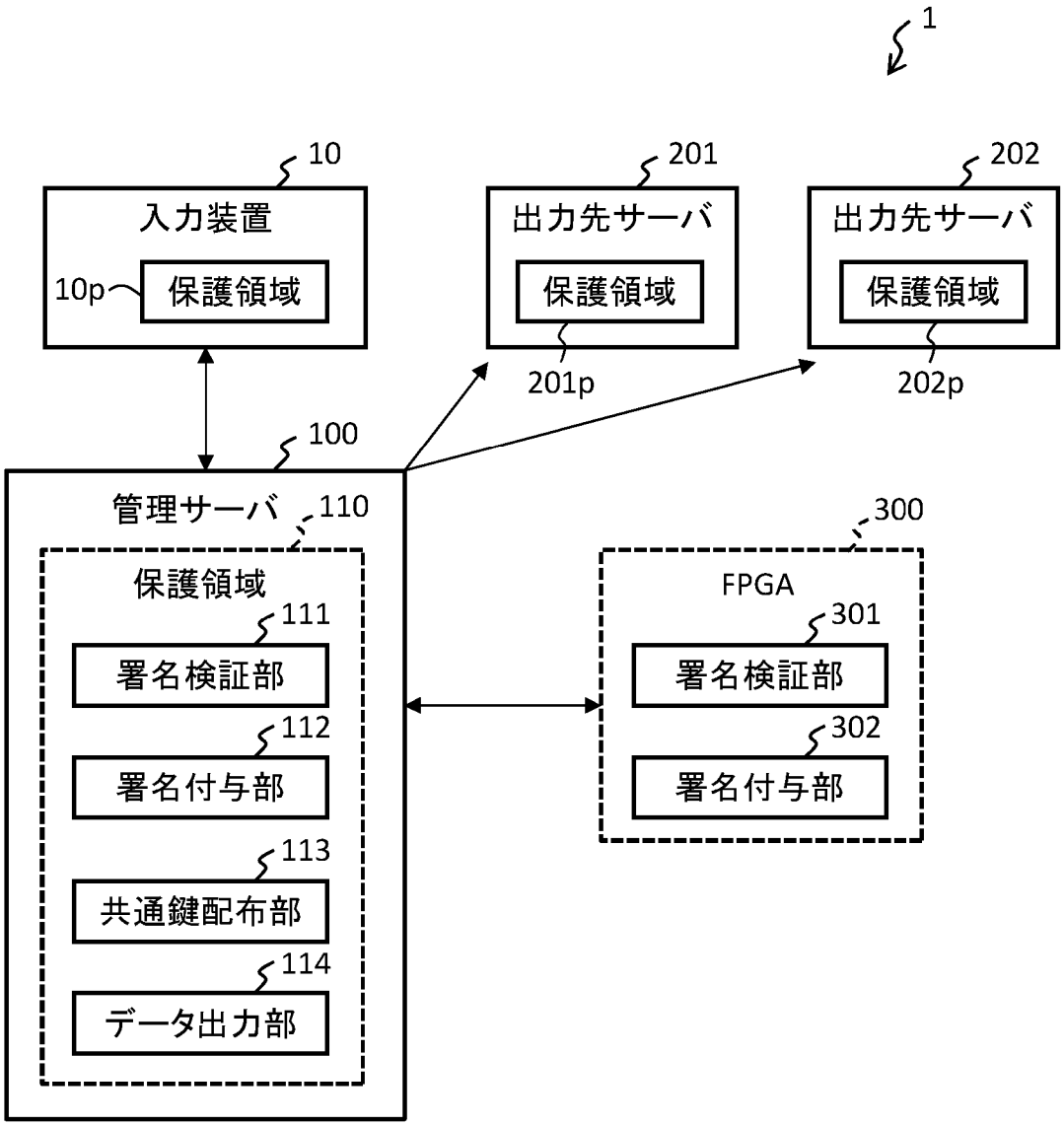
[図3]


110
CK
PK10
PK201
PK202
PK10(CK)
PK201(CK)
PK202(CK)
10
201
202
SK10
SK201
SK202
CK
CK
CK

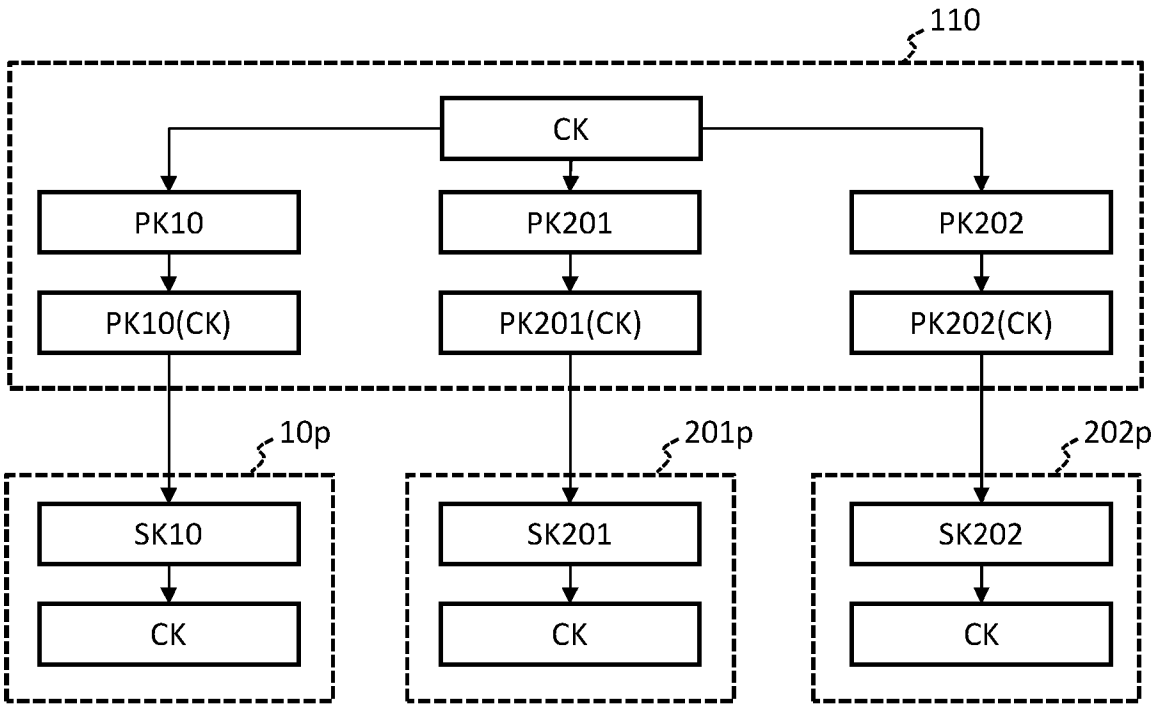
[図4]


110
D2,s300(D2)
CK
CK(D2||s300(D2))
10
201
202
CK
CK
CK
D2||s300(D2)
D2||s300(D2)
D2||s300(D2)

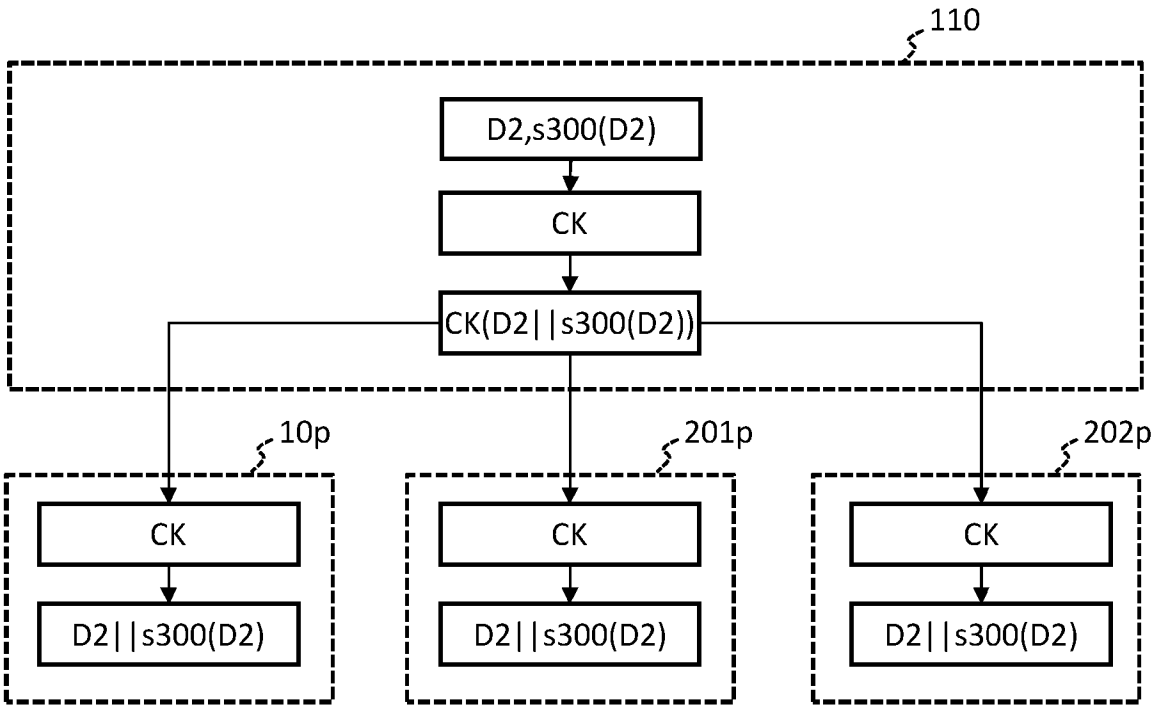
[図5]


1
10
入力装置
10p
保護領域
201
出力先サーバ
保護領域
201p
202
出力先サーバ
保護領域
202p
100
管理サーバ
110
保護領域
111
署名検証部
112
署名付与部
113
共通鍵配布部
114
データ出力部
300
FPGA
301
署名検証部
302
署名付与部

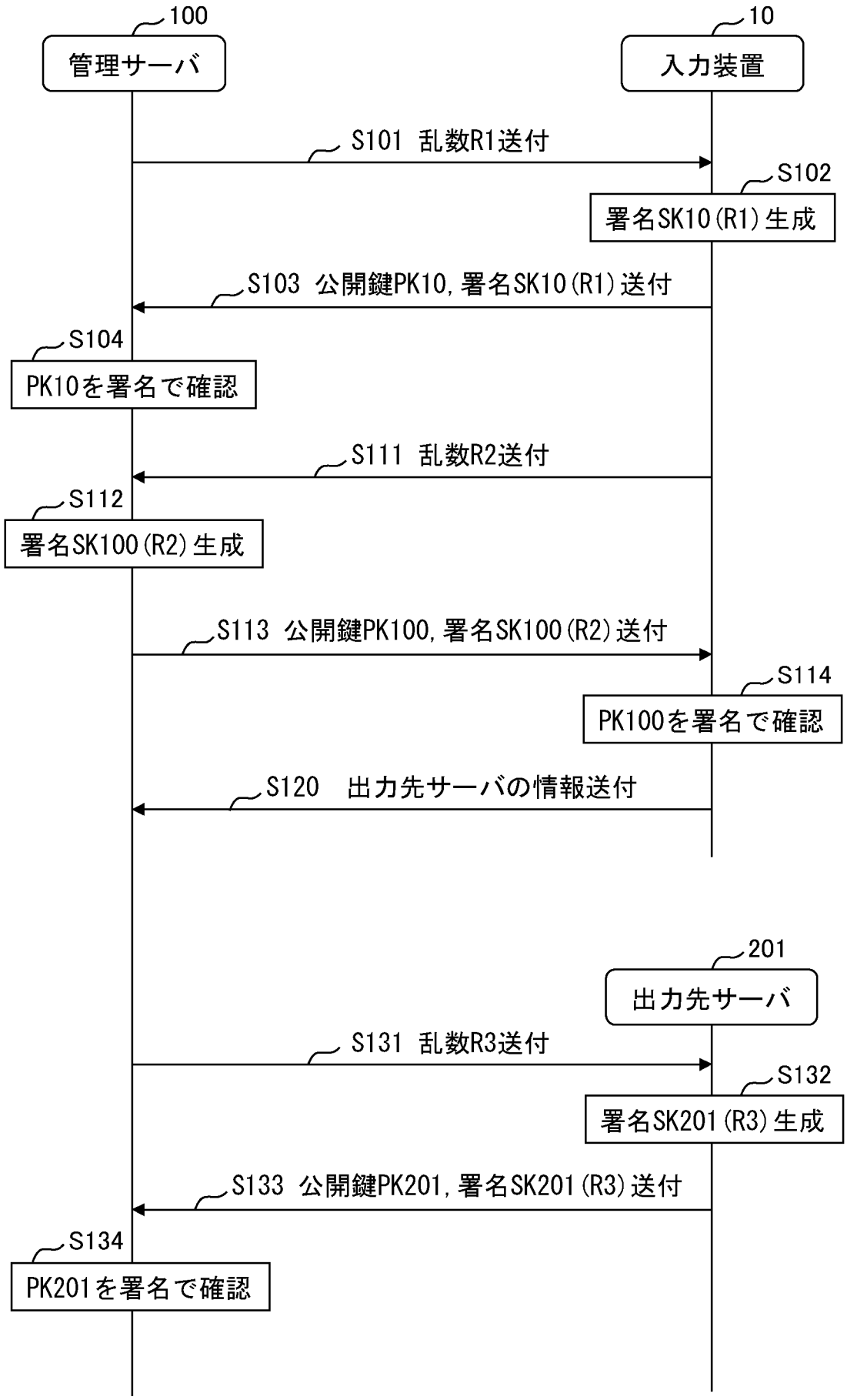
[図6]


110
CK
PK10
PK201
PK202
PK10(CK)
PK201(CK)
PK202(CK)
10p
201p
202p
SK10
SK201
SK202
CK
CK
CK

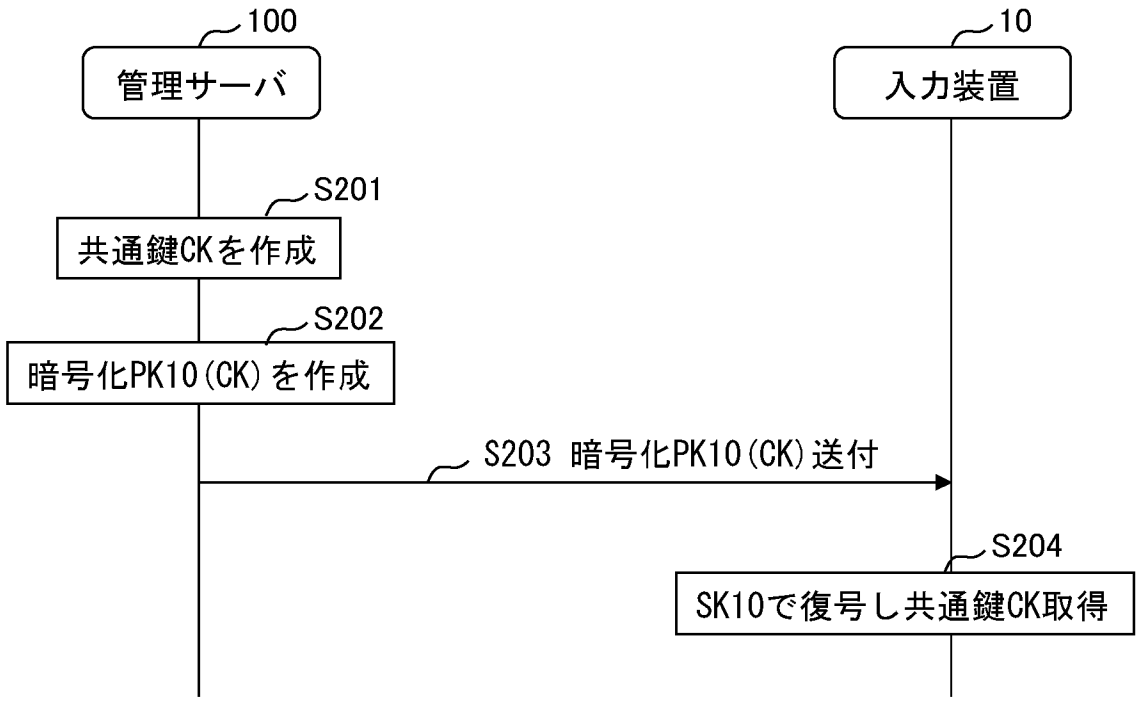
[図7]


110
D2,s300(D2)
CK
CK(D2||s300(D2))
10p
201p
202p
CK
CK
CK
D2||s300(D2)
D2||s300(D2)
D2||s300(D2)

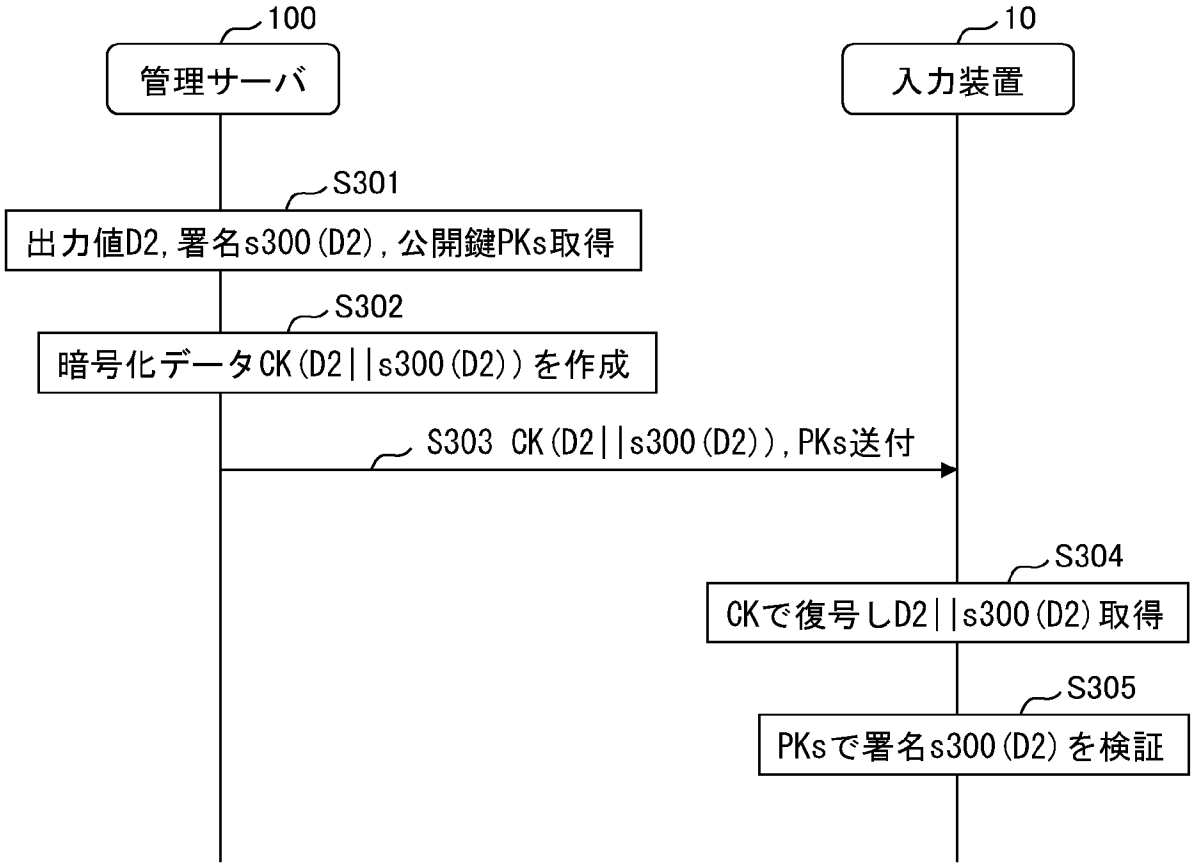
[図8]


100
管理サーバ
10
入力装置
S101 乱数R1送付
S102
署名SK10(R1)生成
S103 公開鍵PK10,署名SK10(R1)送付
S104
PK10を署名で確認
S111 乱数R2送付
S112
署名SK100(R2)生成
S113 公開鍵PK100,署名SK100(R2)送付
S114
PK100を署名で確認
S120 出力先サーバの情報送付
201
出力先サーバ
S131 乱数R3送付
S132
署名SK201(R3)生成
S133 公開鍵PK201,署名SK201(R3)送付
S134
PK201を署名で確認

[図9]


100
管理サーバ
10
入力装置
S201
共通鍵CKを作成
S202
暗号化PK10(CK)を作成
S203 暗号化PK10(CK)送付
S204
SK10で復号し共通鍵CK取得

[図10]


100
管理サーバ
10
入力装置
S301
出力値D2,署名s300(D2),公開鍵PKs取得
S302
暗号化データCK(D2||s300(D2))を作成
S303 CK(D2||s300(D2)),PKs送付
S304
CKで復号しD2||s300(D2)取得
S305
PKsで署名s300(D2)を検証

[図11]

証明書ID	公開鍵	秘密鍵	主体者	発行者	有効期限
C10	PK10	SK10	入力装置10	1（CA）	20220201～20230131
C100	PK100	SK100	管理サーバ100（保護領域110）	1（CA）	20220201～20230131
C201	PK201	SK201	出力先サーバ201	1（CA）	20220201～20230131
C202	PK202	SK202	出力先サーバ202	1（CA）	20220201～20230131

[図12]

主体者	証明書ID	公開鍵	発行者	有効期限	IPアドレス
入力装置10	C10	PK10	1（CA）	20220201～20230131	10.0.0.10
出力先サーバ201	C201	PK201	1（CA）	20220201～20230131	10.0.0.12
出力先サーバ202	C202	PK202	1（CA）	20220201～20230131	10.0.0.13

[図13]

主体者	証明書ID	公開鍵	発行者	有効期限	IPアドレス
管理サーバ100（保護領域110）	C100	PK100	1（CA）	20220201～20230131	10.0.0.11

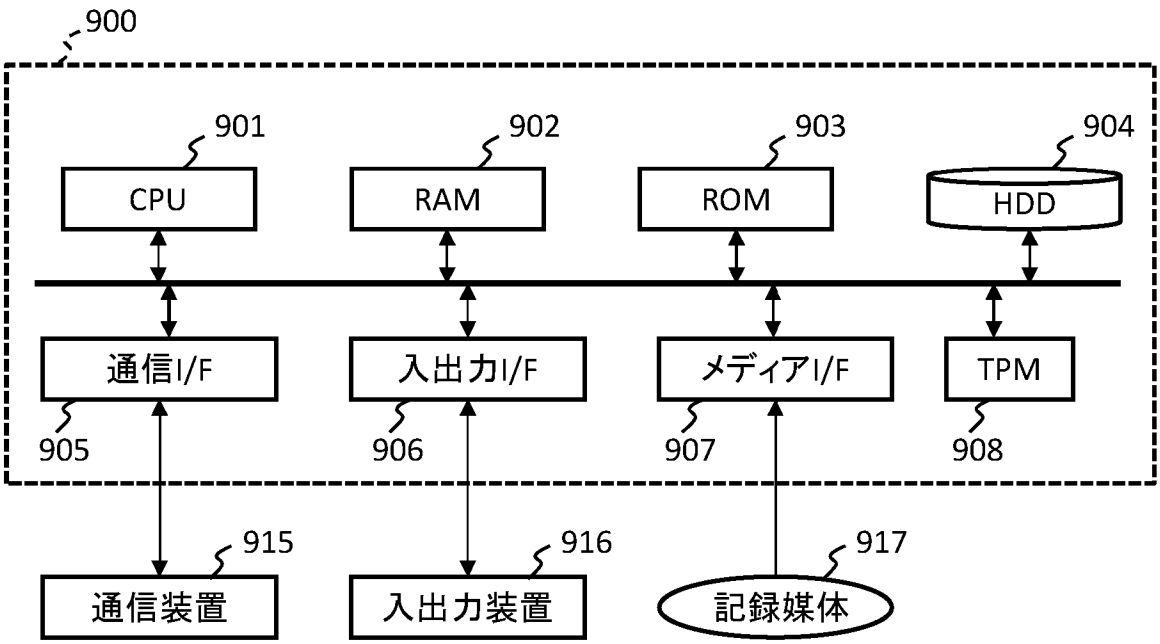
[図14]

要求ID	送付先	送付先証明書	送付先公開鍵	IPアドレス
R01	入力装置10	C10	PK10	10.0.0.10
R01	出力先サーバ201	C201	PK201	10.0.0.12
R01	出力先サーバ202	C202	PK202	10.0.0.13

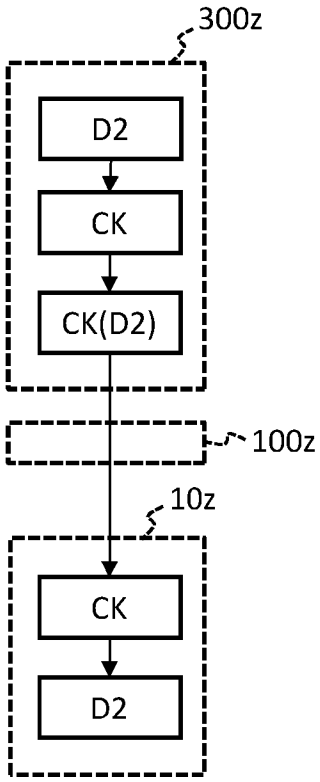
[図15]

主体者	要求ID	共通鍵
管理サーバ100 （保護領域110）	R01	CK

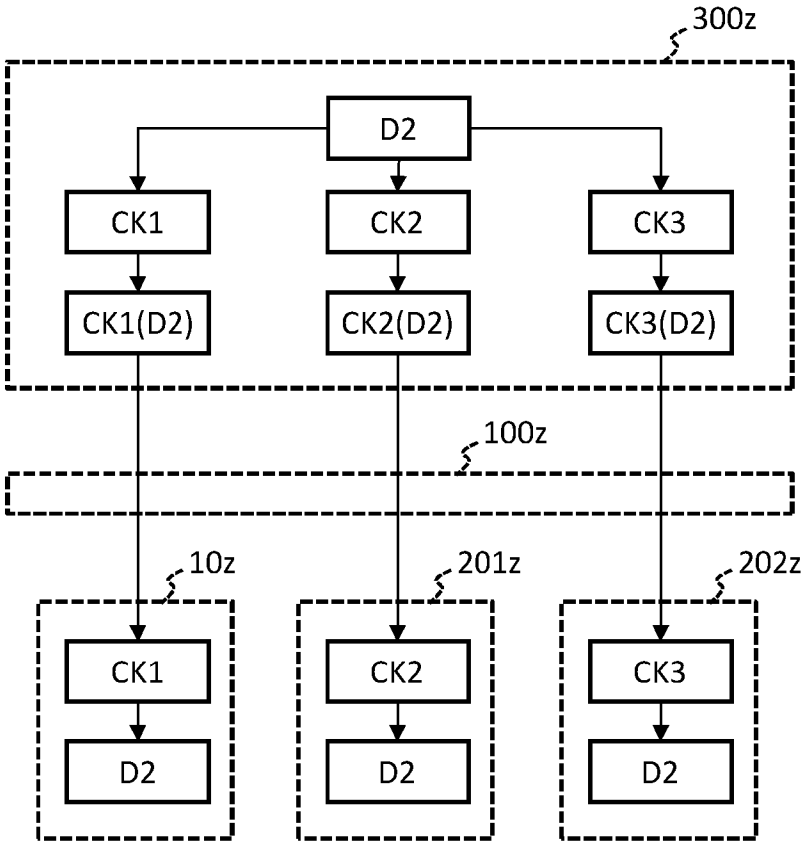
[図16]



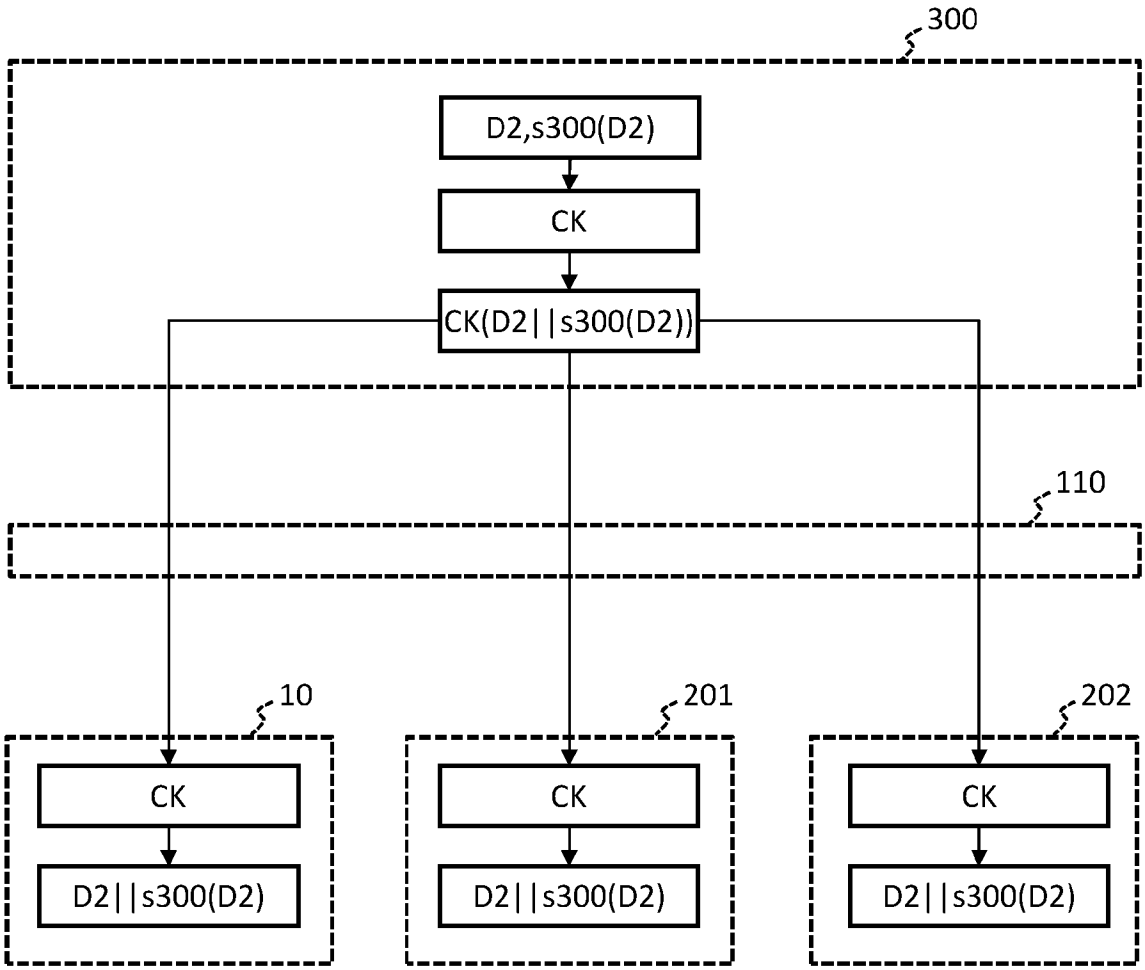
[図17]


300z
D2
CK
CK(D2)
100z
10z
CK
D2

[図18]


300z
D2
CK1
CK2
CK3
CK1(D2)
CK2(D2)
CK3(D2)
100z
10z
201z
202z
CK1
CK2
CK3
D2
D2
D2

[図19]


300
D2,s300(D2)
CK
CK(D2||s300(D2))
110
10
201
202
CK
D2||s300(D2)
CK
D2||s300(D2)
CK
D2||s300(D2)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2022/019759

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i
FI: H04L9/08 B

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)

H04L9/08

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

Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2022
Registered utility model specifications of Japan 1996-2022
Published registered utility model applications of Japan 1994-2022

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.
X	WO 2021/166787 A1 (EAGLYS INC) 26 August 2021 (2021-08-26) paragraphs [0013]-[0082]	1, 5
Y	paragraphs [0013]-[0082]	2
A		3–4
Y	US 2018/0255023 A1 (UNIFYID) 06 September 2018 (2018-09-06) paragraphs [0022]-[0031]	2
A		3–4
A	JP 2020-177223 A (AXELL CORPORATION) 29 October 2020 (2020-10-29)	1-5

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 July 2022	**02 August 2022**
Name and mailing address of the ISA/JP **Japan Patent Office (ISA/JP)** **3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915** **Japan**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2022/019759

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2021/166787 A1	26 August 2021	(Family: none)	
US 2018/0255023 A1	06 September 2018	(Family: none)	
JP 2020-177223 A	29 October 2020	US 2020/0328882 A1	

国際調査報告

国際出願番号
PCT/JP2022/019759

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/08(2006.01)i
FI: H04L9/08 B

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２２年
日本国実用新案登録公報	１９９６－２０２２年
日本国登録実用新案公報	１９９４－２０２２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
X	WO 2021/166787 A1 (ＥＡＧＬＹＳ株式会社) 26.08.2021 (2021-08-26) 段落[0013]-[0082]	1, 5
Y	段落[0013]-[0082]	2
A		3-4
Y	US 2018/0255023 A1 (UNIFYID) 06.09.2018 (2018-09-06) 段落[0022]-[0031]	2
A		3-4
A	JP 2020-177223 A (株式会社アクセル) 29.10.2020 (2020-10-29)	1-5

☐ 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抵触するものではなく、発明の原理又は理論の理解のために引用するもの
“X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
“Y” 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
“&” 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
22.07.2022	02.08.2022

名称及びあて先

日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）

打出　義尚 5S 4440

電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2022/019759

引用文献	公表日	パテントファミリー文献	公表日
WO 2021/166787 A1	26.08.2021	（ファミリーなし）	
US 2018/0255023 A1	06.09.2018	（ファミリーなし）	
JP 2020-177223 A	29.10.2020	US 2020/0328882 A1	