

(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
2019年10月17日(17.10.2019)



(10) 国際公開番号

WO 2019/198516 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2019/013412

(22) 国際出願日: 2019年3月27日(27.03.2019)

(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 2018-076343 2018年4月11日(11.04.2018) JP

(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: 岡野 裕樹(OKANO, Yuki); 〒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). 吉田 麗生(YOSHIDA, Reo); 〒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). 小林 鉄太郎(KOBAYASHI, Tetsutaro); 〒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: 伊東 忠重, 外(ITO, Tadashige et al.); 〒1000005 東京都千代田区丸の内二丁目1番1号 丸の内 M Y P L A Z A (明治安田生命ビル) 16階 Tokyo (JP).

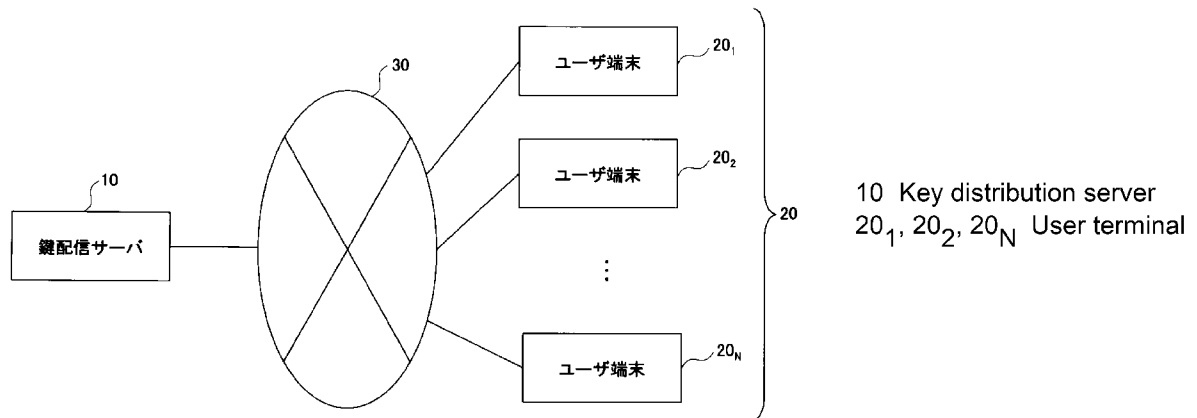
(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ,

(54) **Title:** KEY DISTRIBUTION SYSTEM, TERMINAL DEVICE, KEY DISTRIBUTION METHOD, AND PROGRAM

(54) 発明の名称: 鍵配信システム、端末装置、鍵配信方法、及びプログラム

[図1]

1



(57) **Abstract:** A key distribution system including an N number of terminal devices U_i and a key distribution server used for session key exchanges. The key distribution system has: an isogenic calculation means whereby, if N is an even number, an odd-numbered terminal device U_i uses a base of a first twisted section group having a prescribed elliptical curve and calculates a first public value and an even-numbered terminal device U_i uses a base of a second twisted section group having said elliptical curve and calculates a second public value; a distribution means whereby the key distribution server distributes the first public value calculated by the odd-numbered terminal device U_i to terminal device U_{i-1} and terminal device U_{i+1} and the distributes the second public value calculated by the even-numbered terminal device U_i to terminal device U_{i-1} and terminal device U_{i+1} ; and a key generation means that whereby the odd-numbered terminal device U_i uses the second public value distributed

[続葉有]



WO 2019/198516 A1

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, IR, IS, JO, JP, KE, KG, KH, 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, 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, RW, 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))

by the distribution means and generates the session key and the even-numbered terminal device U_i uses the first public value distributed by the distribution means and generates the session key. The key distribution system is characterized by the isogenic calculation means calculating the first public value for which a prescribed terminal device U_i among the terminal devices U_i uses the first twisted section group base and calculating the second public value using the second twisted section group base, if N is odd.

(57) 要約: N 台の端末装置 U_i と、セッション鍵の交換に用いられる鍵配信サーバとが含まれる鍵配信システムであって、 N が偶数である場合、奇数番目の端末装置 U_i が所定の楕円曲線の第1のねじれ部分群の基底を用いた第1の公開値を計算し、偶数番目の端末装置 U_i が前記楕円曲線の第2のねじれ部分群の基底を用いた第2の公開値を計算する同種写像計算手段と、前記鍵配信サーバが、奇数番目の端末装置 U_i により計算された第1の公開値を端末装置 U_{i-1} 及び端末装置 U_{i+1} に配信し、偶数番目の端末装置 U_i により計算された第2の公開値を端末装置 U_{i-1} 及び端末装置 U_{i+1} に配信する配信手段と、前記配信手段により配信された第2の公開値を用いて奇数番目の端末装置 U_i が前記セッション鍵を生成し、前記配信手段により配信された第1の公開値を用いて偶数番目の端末装置 U_i が前記セッション鍵を生成する鍵生成手段と、を有し、前記同種写像計算手段は、 N が奇数である場合、前記端末装置 U_i のうち、所定の端末装置 U_i が前記第1のねじれ部分群の基底を用いた第1の公開値と、前記第2のねじれ部分群の基底を用いた第2の公開値とを計算する、ことを特徴とする鍵配信システム。

明 細 書

発明の名称：

鍵配信システム、端末装置、鍵配信方法、及びプログラム

技術分野

[0001] 本発明は、鍵配信システム、端末装置、鍵配信方法、及びプログラムに関する。

背景技術

[0002] スマートフォンやタブレット端末等の各種ユーザ端末の普及に伴って、何等かのデータをサーバに預託することで、このデータを多人数で共有するようなサービスが増えてきた。このようなサービスとしては、例えば、オンラインストレージサービス、グループチャットサービス、グループメールサービス等が挙げられる。

[0003] 上記のようなサービスを提供するシステムでは、例えば、通信路を暗号化することで通信経路上の盗聴防止が施されていたり、ユーザ端末にデータを残さないことによってユーザ端末の紛失や不正な持ち出しに起因する情報漏えい防止が施されていたりする。このように、上記のようなサービスを提供するシステムでは、通信経路に対する脅威（例えば、盗聴等）やユーザ端末に対する脅威（例えば、紛失や不正な持ち出し等）に対処が行われている場合が多い。

[0004] ここで、上記のようなサービスを提供するシステムにおいては、サーバに対する脅威に起因する情報漏えいの恐れも考えられる。サーバに対する脅威には、例えば、サーバに対する外部からの攻撃やサーバ管理者等による内部不正等がある。これらの脅威に起因する情報漏えいを防止する方法として、例えば、サーバに対してはデータを秘匿化し、ユーザ端末でのみデータの復号可能なエンドツーエンド暗号化を行う方法がある。

[0005] エンドツーエンド暗号化では、ユーザ端末間で用いる共通鍵をどのように共有するかが問題となる。これに対して、多者間鍵交換技術の1つとして、

中央に認証サーバが配置されたスター型のネットワークにおいて、認証サーバに対していかなる情報も漏らさずにユーザ端末間で鍵（以下「セッション鍵」と表す。）を共有することが可能な動的多者鍵配布（DMKD : Dynamic Multi-Cast Key Distribution）プロトコルが知られている。DMKDプロトコルによって、認証サーバに対してデータの内容を秘匿したままユーザ端末間でデータの送受信を行うことができるようになる。また、DMKDプロトコルでは、データの送受信を行う複数のユーザ端末間でのみセッション鍵の共有を行うため、例えば、これらの複数のユーザ端末に対して新たなユーザ端末が追加された場合やこれらの複数のユーザ端末から或るユーザ端末が離脱した場合等にはセッション鍵が更新される。

[0006] ところで、以下の参考文献1では、DH (Diffie-Hellman) 鍵交換を用いたDMKDプロトコルが提案されている。

[0007] [参考文献1]

K. Yoneyama, R. Yoshida, Y. Kawahara, T. Kobayashi, H. Fuji, and T. Yamamoto. 2016. Multi-Cast Key Distribution: Scalable, Dynamic and Provably Secure Construction. Cryptology ePrint Archive, Report 2016/833. (2016).

しかしながら、参考文献1で提案されているDMKDプロトコルは、DH鍵交換を用いているため、耐量子性がないことが知られている。このため、今後、量子コンピュータの実用化が進むにつれて、計算量仮定であるCDH (Computational Diffie-Hellman)・DDH (Decisional Diffie-Hellman) 問題が効率よく解かれてしまい、鍵共有の安全性が担保されない可能性がある。これに対して、鍵カプセル化メカニズム (KEM : Key Encapsulation Mechanism) を用いることで、格子暗号や符号ベース暗号等の耐量子暗号に適用可能なDMKDプロトコルが提案されている（非特許文献1）。

先行技術文献

非特許文献

[0008] 非特許文献1：金城皓羽、岡野裕樹、斉藤恒和、草川恵太、小林鉄太郎、星野

文学、「KEMを用いた動的多者鍵配布プロトコル」、SCIS2018

発明の概要

発明が解決しようとする課題

[0009] しかしながら、非特許文献1で提案されている手法は耐量子があるものの、鍵カプセル化メカニズムを用いているため、DH鍵交換を用いたDMKDプロトコルよりも1ラウンド多い通信が必要である。このため、非特許文献1で提案されている手法は、DH鍵交換を用いたDMKDプロトコルよりも余分な通信コストが必要であった。

[0010] 本発明は、上記の点に鑑みてなされたもので、耐量子性があり、かつ、通信コストが少ない多者間鍵交換を実現することを目的とする。

課題を解決するための手段

[0011] 上記目的を達成するため、本発明の実施の形態は、 N （ただし、 $N \geq 2$ ）台の端末装置 U_i （ $i = 1, \dots, N$ ）と、該 N 台の端末装置 U_i 間で同種写像暗号によるセッション鍵の交換に用いられる鍵配信サーバとが含まれる鍵配信システムであって、 N が偶数である場合、前記端末装置 U_i のうち、奇数番目の端末装置 U_i （ $i = 1, \dots, N-1$ ）が所定の楕円曲線の第1のねじれ部分群の基底を用いた第1の公開値を計算し、偶数番目の端末装置 U_i （ $i = 2, \dots, N$ ）が前記楕円曲線の第2のねじれ部分群の基底を用いた第2の公開値を計算する同種写像計算手段と、前記鍵配信サーバが、奇数番目の端末装置 U_i により計算された第1の公開値を端末装置 U_{i-1} （ただし、 $i = 1$ である場合、 $U_0 = U_N$ ）及び端末装置 U_{i+1} （ただし、 $i = N$ である場合、 $U_{N+1} = U_1$ ）に配信し、偶数番目の端末装置 U_i により計算された第2の公開値を端末装置 U_{i-1} 及び端末装置 U_{i+1} に配信する配信手段と、前記配信手段により配信された第2の公開値を用いて奇数番目の端末装置 U_i が前記セッション鍵を生成し、前記配信手段により配信された第1の公開値を用いて偶数番目の端末装置 U_i が前記セッション鍵を生成する鍵生成手段と、を有し、前記同種写像計算手段は、 N が奇数である場合、前記端末装置 U_i のうち、予め決められた所定の端末装置 U_i が前記第1のねじれ部分群の基底を用い

た第１の公開値と、前記第２のねじれ部分群の基底を用いた第２の公開値とを計算する、ことを特徴とする。

発明の効果

[0012] 本発明によれば、耐量子性があり、かつ、通信コストが少ない多者間鍵交換を実現することができる。

図面の簡単な説明

[0013] [図1]本発明の実施の形態における鍵交換システムのシステム構成の一例を示す図である。

[図2]本発明の実施の形態における鍵配信サーバの機能構成の一例を示す図である。

[図3]本発明の実施の形態におけるユーザ端末の機能構成の一例を示す図である。

[図4]本発明の実施の形態における鍵交換システムの事前処理の流れの一例を説明するための図である。

[図5]本発明の実施の形態における鍵交換システムの鍵交換処理の流れの一例を説明するための図である。

[図6]本発明の実施の形態における鍵配信サーバ及びユーザ端末のハードウェア構成の一例を示す図である。

発明を実施するための形態

[0014] 以下、本発明の実施の形態について説明する。本発明の実施の形態では、耐量子暗号として同種写像暗号を用いて、非特許文献１で提案されている手法よりも少ないラウンド（２ラウンド）の通信で多者間鍵交換を行う鍵交換システム１について説明する。

[0015] <システム構成>

図１に示すように、本発明の実施の形態における鍵交換システム１には、鍵配信サーバ１０と、複数のユーザ端末２０とが含まれる。鍵配信サーバ１０と各ユーザ端末２０とは、例えばインターネット等のネットワーク３０を介して通信可能に接続されている。

[0016] 鍵配信サーバ10は、各ユーザ端末20間で共通鍵を共有するために、各ユーザ端末20の公開鍵の配信を行うサーバである。鍵配信サーバ10は、1台の情報処理装置（コンピュータ）又は複数台の情報処理装置で実現される。

[0017] ユーザ端末20は、本発明の実施の形態における鍵交換システム1に登録されているユーザが利用する端末である。各ユーザ端末20は、鍵配信サーバ10を介して、他のユーザ端末20との間で公開鍵を交換することで、共通鍵を共有することができる。ユーザ端末20としては、例えば、スマートフォンやタブレット端末、PC（パーソナルコンピュータ）、ウェアラブルデバイス、ゲーム機器、家電製品、組み込み機器等の種々の情報処理装置を用いることができる。

[0018] 本発明の実施の形態では、鍵交換システム1に登録されているユーザのうち、鍵交換を行うユーザの数をNとし、これらのユーザが利用するユーザ端末20をそれぞれ「ユーザ端末20₁」、「ユーザ端末20₂」、・・・、「ユーザ端末20_N」と表す。したがって、本発明の実施の形態では、各ユーザ端末20_i（1 ≤ i ≤ N）をそれぞれ表す記号として、添え字i（1 ≤ i ≤ N）を用いる。また、本発明の実施の形態では、鍵配信サーバ10を表す記号として、Sを用いる。

[0019] <定義>

ここで、本発明の実施の形態で用いる記号等を定義する。

[0020] 整数をnとして、整数環Zに対するnを法とする剰余環（又は剰余類環）をZ/nZとする。

[0021] また、1以上の整数fを、

[0022] [数1]

$$l_A^{e_A} l_B^{e_B} \cdot f + 1$$

又は

[0023] [数2]

$$l_A^{e_A} l_B^{e_B} \cdot f - 1$$

が素数となるように選択する。ここで、 l_A 及び l_B は小さい素数（例えば、2及び3）であり、 e_A 及び e_B は整数である。

[0024] [数3]

$$l_A^{e_A} l_B^{e_B} \cdot f + 1$$

又は

[0025] [数4]

$$l_A^{e_A} l_B^{e_B} \cdot f - 1$$

が素数である場合、これらのうち素数である方（両方が素数である場合は任意に選んだ何れか一方）を p と表す。

[0026] また、

[0027] [数5]

$$\mathbf{F}_{p^2}$$

を標数 p の素体 F_p の 2 次拡大体とする。 E を

[0028] [数6]

$$\mathbf{F}_{p^2}$$

上の楕円曲線とする。例えば、

[0029] [数7]

$$E = \left\{ (x, y) \in \mathbf{F}_{p^2}^2 \mid y^2 = x^3 + ax + b, \ a, b \in \mathbf{F}_{p^2}, \ 4a^3 + 27b^2 \neq 0 \right\} \cup \{O\}$$

とすると、 E は

[0030] [数8]

$$\mathbf{F}_{p^2}$$

上の楕円曲線である。ここで、 O は無限遠点である。以降、本発明の実施の形態では、楕円曲線 E は超特異楕円曲線であるものとする。

[0031] 楕円曲線 E の j 不変量を、

[0032] [数9]

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

とする。楕円曲線 E の任意の点 P と任意の整数 m とに対して、 P の m 個の和を $[m] P$ と表す。ただし、和は、楕円曲線上の加算である。

[0033] 整数 m に対して、楕円曲線 E の m ねじれ部分群 $E[m]$ を、 $E[m] = \{P \in E \mid [m] P = O\}$ と定義する。 m ねじれ部分群 $E[m]$ は、 p で割り切れない整数 m に対して、

[0034] [数10]

$$E[m] \simeq \mathbf{Z} / m\mathbf{Z} \times \mathbf{Z} / m\mathbf{Z}$$

であることが知られている。ここで、

[0035] [数11]

$$A \simeq B$$

は2つの群 A 及び B の間に同型写像が存在することを意味する。

[0036] 本発明の実施の形態では、 k をセキュリティパラメータ、シード $s \in \{0, 1\}^k$ をインデックスとし、定義域 Dom_k と値域 Rng_k とを持つ関数族 $\{F_s : \text{Dom}_k \rightarrow \text{Rng}_k\}_s$ のうち、疑似ランダム関数と呼ばれる関数を使用する。また、本発明の実施の形態では、この疑似ランダム関数によるねじれ疑似ランダム関数 $tPRF$ を使用する。なお、ねじれ疑似ランダム関数 $tPRF$ は、入力の一部が知られたとしても、その関数の出力がランダム値と区別が困難であるという性質を有する関数である。

[0037] なお、ねじれ疑似ランダム関数については、例えば、以下の参考文献2に開示されている。

[0038] [参考文献2]

K. Yoneyama, R. Yoshida, Y. Kawahara, T. Kobayashi, H. Fuji, and T. Yamamoto. 2016. Multi-Cast Key Distribution: Scalable, Dynamic and Provably Secure Construction. Cryptology ePrint Archive, Report 2016/833. (2016).

<機能構成>

図2に示すように、本発明の実施の形態における鍵配信サーバ10は、機能部として、セットアップ部101と、長期秘密ストリング生成部102と、短期秘密ストリング生成部103と、公開情報計算部104と、通信部105と、長期秘密ストリング記憶部106と、短期秘密ストリング記憶部107とを有する。これらの各機能部によって、鍵配信サーバ10は、後述する事前処理（図4）及び鍵交換処理（図5）を実現することができる。

[0039] また、図3に示すように、本発明の実施の形態におけるユーザ端末20は、機能部として、長期秘密ストリング生成部201と、短期秘密ストリング生成部202と、ねじれ疑似ランダム関数部203と、同種写像計算部204と、第1疑似ランダム関数部205と、秘密情報計算部206と、第2疑似ランダム関数部207と、通信部208と、長期秘密ストリング記憶部209と、短期秘密ストリング記憶部210と、セッション情報記憶部211とを有する。これら各機能部によって、各ユーザ端末20は、後述する事前処理（図4）及び鍵交換処理（図5）を実現することができる。

[0040] <事前処理>

次に、本発明の実施の形態における鍵交換システム1の事前処理の流れについて、図4を参照しながら説明する。図4は、本発明の実施の形態における鍵交換システム1の事前処理の流れの一例を説明するための図である。なお、セキュリティパラメータ k は予め決められているものとする。例えば、 $k = 256$ 等決められているものとする。

[0041] ステップS101：鍵配信サーバ10のセットアップステップ

鍵配信サーバ10のセットアップ部101は、 k ビットの数

[0042]

[数12]

$$p = l_A^{e_A} l_B^{e_B} \cdot f \pm 1$$

が素数となるように整数 f を選択する。ここで、 l_A 及び l_B は素数、 e_A 及び e_B は整数である。

[0043] また、鍵配信サーバ 10 のセットアップ部 101 は、

[0044] [数13]

$$\mathbf{F}_{p^2}$$

上の超特異楕円曲線 E を生成し、

[0045] [数14]

$$E \text{ の } l_A^{e_A} \text{ ねじれ部分群 } E[l_A^{e_A}] \text{ の基底 } \{P_A, Q_A\}$$

と

[0046] [数15]

$$E \text{ の } l_B^{e_B} \text{ ねじれ部分群 } E[l_B^{e_B}] \text{ の基底 } \{P_B, Q_B\}$$

とを選択する。基底の選択方法は、例えば、以下の参考文献 3 に開示されている方法を用いることができる。

[0047] [参考文献3]

L. De Feo, D. Jao, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, In PQCrypto, pp.19-34, 2011.

更に、鍵配信サーバ10のセットアップ部101は、 $Kspace_k$ を鍵空間とし、以下のねじれ疑似ランダム関数 $tPRF_A$ 、 $tPRF_B$ 及び $tPRF$ を生成する。

[0048] [数16]

$$\begin{aligned} tPRF_A: \{0,1\}^k \times Kspace_k \times \{0,1\}^k \times Kspace_k &\rightarrow \mathbf{Z} / l_A^{e_A} \mathbf{Z} \\ tPRF_B: \{0,1\}^k \times Kspace_k \times \{0,1\}^k \times Kspace_k &\rightarrow \mathbf{Z} / l_B^{e_B} \mathbf{Z} \\ tPRF: \{0,1\}^k \times Kspace_k \times \{0,1\}^k \times Kspace_k &\rightarrow \{0,1\}^k \end{aligned}$$

また、鍵配信サーバ10のセットアップ部101は、以下の疑似ランダム関数 F 及び F' を生成する。

[0049] [数17]

$$\begin{aligned} F: \{0,1\}^k \times \mathbf{F}_{p^2} &\rightarrow \{0,1\}^k \\ F': \{0,1\}^k \times \{0,1\}^k &\rightarrow Kspace_k \end{aligned}$$

そして、鍵配信サーバ10のセットアップ部101は、 $(p, l_A, e_A, l_B, e_B, E, P_A, Q_A, P_B, Q_B, tPRF_A, tPRF_B, tPRF, F, F')$ を公開する。これにより、各ユーザ端末20は、これらの公開された情報を利用することができる。

[0050] ステップS102：鍵配信サーバ10の長期秘密ストリング生成ステップ

鍵配信サーバ10の長期秘密ストリング生成部102は、長期秘密ストリングとして、 $st_s \in Kspace_k$ と、 $st'_s \in \{0, 1\}^k$ とを一様ランダムに生成する。そして、鍵配信サーバ10の長期秘密ストリング生成部1

02は、生成した長期秘密ストリング (st_s , st'_s) を長期秘密ストリング記憶部106に保存する。

[0051] ステップS103: 各ユーザ端末20の長期秘密ストリング生成ステップ
各ユーザ端末20の長期秘密ストリング生成部201は、長期秘密ストリングとして、 $st_i \in Kspace_k$ と、 $st'_i \in \{0, 1\}^k$ とを一様ランダムに生成する。なお、 st_i 及び st'_i は、ユーザ端末20_iの長期秘密ストリング生成部201により生成された長期秘密ストリングである。

[0052] そして、各ユーザ端末20の長期秘密ストリング生成部201は、生成した長期秘密ストリング (st_i , st'_i) を、自身の長期秘密ストリング記憶部209に保存する。

[0053] <鍵交換処理>

次に、本発明の実施の形態における鍵交換システム1の鍵交換処理の流れについて、図5を参照しながら説明する。図5は、本発明の実施の形態における鍵交換システム1の鍵交換処理の流れの一例を説明するための図である。

[0054] 以降で説明する鍵交換処理は、鍵交換システム1の動作中に任意の回数実行が可能である。1回あたりの鍵交換の実行を「セッション」と呼ぶ。以降では、或るセッションにおける鍵配信サーバ10及び各ユーザ端末20の動作を説明する。なお、当該セッションを識別するセッション識別子を $sid \in \{0, 1\}^k$ とする。セッション識別子 sid の生成方法としては、任意の方法を用いることができる。例えば、非特許文献1に開示されているように、コミットメントを用いて生成する方法が挙げられる。鍵配信サーバ10及び各ユーザ端末20は、この sid を知っているものとする。

[0055] また、各ユーザ端末20の中で代表となるユーザ端末20（代表ユーザ端末）を決めておく。ユーザ端末20₁、ユーザ端末20₂、・・・、ユーザ端末20_Nのうち、任意のユーザ端末20を代表ユーザ端末として良い。以降では、ユーザ端末20₁が代表ユーザ端末であるものとする。代表ユーザ端末の選択及び代表ユーザ端末であることを示す通知は、例えば、鍵配信サーバ1

0により行われても良い。

[0056] また、ユーザ端末20の添え字 i はリング状であるものとする。すなわち、 $i = N$ に対して1が加算された場合 $i = 1$ となり、 $i = 1$ から -1 が減算された場合 $i = N$ となるものとする。

[0057] ここで、同種写像暗号では、DH鍵交換と異なり、或る2つのユーザ端末20において、基底 $\{P_A, Q_A\}$ から秘密鍵を生成するか又は基底 $\{P_B, Q_B\}$ から秘密鍵を生成するかのいずれかによって計算の非対称性が生じる。

[0058] このため、実施例1では、ユーザ端末20の数 N の偶奇によって代表ユーザ端末の処理が異なる場合について説明する。すなわち、実施例1では、 N が偶数である場合は、ユーザ端末20₁、ユーザ端末20₃、 $\dots$ 、ユーザ端末20 _{$N-1$} は基底 $\{P_A, Q_A\}$ からそれぞれ公開値を計算し、ユーザ端末20₂、ユーザ端末20₄、 $\dots$ 、ユーザ端末20 _{N} は基底 $\{P_B, Q_B\}$ からそれぞれ公開値を計算する。一方で、 N が奇数である場合は、代表ユーザ端末であるユーザ端末20₁は基底 $\{P_A, Q_A\}$ 及び基底 $\{P_B, Q_B\}$ の両方からそれぞれ公開値を計算し、ユーザ端末20₃、ユーザ端末20₅、 $\dots$ 、ユーザ端末20 _{$N-1$} は基底 $\{P_A, Q_A\}$ からそれぞれ公開値を計算し、ユーザ端末20₂、ユーザ端末20₄、 $\dots$ 、ユーザ端末20 _{N} は基底 $\{P_B, Q_B\}$ からそれぞれ公開値を計算する。なお、公開値には、後述する $\phi_i(P_A)$ 、 $\phi_i(Q_A)$ 、 $\phi_i(P_B)$ 、 $\phi_i(Q_B)$ が含まれる。

[0059] また、実施例2では、ユーザ端末20の数 N の偶奇によらずに、全てのユーザ端末20が基底 $\{P_A, Q_A\}$ 及び基底 $\{P_B, Q_B\}$ の両方からそれぞれ共通鍵を生成する場合について説明する。

[0060] (実施例1)

以降では、実施例1について説明する。

[0061] ≪ N が偶数である場合≫

まず、 N が偶数である場合について説明する。

[0062] ステップS201：第一鍵生成ステップ(Round1)

以降のS201-11~S201-15は、 i が奇数である各ユーザ端末

20_i (i = 1, 3, ..., N-1) が実行する。

[0063] S201-11) 短期秘密ストリング生成部202は、短期秘密ストリングとして、 $r_i^{(1)} \in \{0, 1\}^k$ と、 $r_i^{(2)} \in \text{Kspace}_k$ と、 $r_i^{(3)} \in \{0, 1\}^k$ と、 $r_i^{(4)} \in \text{Kspace}_k$ と、 $k_i^{(1)} \in \{0, 1\}^k$ と、 $k_i^{(2)} \in \text{Kspace}_k$ とを一様ランダムに生成する。

[0064] そして、短期秘密ストリング生成部202は、短期秘密ストリング($r_i^{(1)}$, $r_i^{(2)}$, $r_i^{(3)}$, $r_i^{(4)}$, $k_i^{(1)}$, $k_i^{(2)}$)を短期秘密ストリング記憶部210に保存する。

[0065] S201-12) ねじれ疑似ランダム関数部203は、 $m_i = \text{tPRF}_A(r_i^{(1)}, r_i^{(2)}, st_i, st'_i)$ と、 $n_i = \text{tPRF}_A(r_i^{(3)}, r_i^{(4)}, st_i, st'_i)$ と、 $k_i = \text{tPRF}(k_i^{(1)}, k_i^{(2)}, st_i, st'_i)$ とを生成する。なお、長期秘密ストリング(st_i, st'_i)は、長期秘密ストリング記憶部209は記憶されているものを使用する。

[0066] S201-13) 同種写像計算部204は、 $[m_i]P_A + [n_i]Q_A$ で生成されるEの部分群 K_i を核に持つ同種写像 $\phi_i: E \rightarrow E_i$ と、この同種写像 ϕ_i に付随する楕円曲線 E_i とを計算する。

[0067] なお、部分群 K_i を核に持つ同種写像 ϕ_i とは、 $\text{Ker } \phi_i = K_i$ となる同種写像のことである。このような同種写像 ϕ_i と部分群 K_i とは1対1に対応することが知られている。また、同種写像 ϕ_i に付随する楕円曲線 E_i は、 $E_i = E/K_i$ とも表される。同種写像 ϕ_i の計算方法は、例えば、以下の参考文献4又は5に開示されている方法を用いることができる。

[0068] [参考文献4]

J. Velu, Isogenies entre courbes elliptiques, C. R. Acad. Sci. Paris Ser. A-B, 273:A238-241, 1971.

[参考文献5]

Lawrence C. Washington. Elliptic curves: Number theory and cryptography, 2nd ed., CRC Press, 2008.

S201-14) 同種写像計算部204は、 $\phi_i(P_B)$ と $\phi_i(Q_B)$ とを

計算する。

[0069] S 2 0 1 - 1 5) そして、通信部 2 0 8 は、 $(\phi_i(P_B), \phi_i(Q_B), E_i)$ を鍵配信サーバ 1 0 に送信する。これより、各ユーザ端末 2 0 $_i$ ($i = 1, 3, \dots, N-1$) の公開値 $(\phi_i(P_B), \phi_i(Q_B), E_i)$ が鍵配信サーバ 1 0 に送信される。

[0070] 以降の S 2 0 1 - 2 1 ~ S 2 0 1 - 2 5 は、 i が偶数である各ユーザ端末 2 0 $_i$ ($i = 2, 4, \dots, N$) が実行する。

[0071] S 2 0 1 - 2 1) 短期秘密ストリング生成部 2 0 2 は、短期秘密ストリングとして、 $r_i^{(1)} \in \{0, 1\}^k$ と、 $r_i^{(2)} \in \text{Kspace}_k$ と、 $r_i^{(3)} \in \{0, 1\}^k$ と、 $r_i^{(4)} \in \text{Kspace}_k$ と、 $k_i^{(1)} \in \{0, 1\}^k$ と、 $k_i^{(2)} \in \text{Kspace}_k$ とを一様ランダムに生成する。

[0072] そして、短期秘密ストリング生成部 2 0 2 は、短期秘密ストリング $(r_i^{(1)}, r_i^{(2)}, r_i^{(3)}, r_i^{(4)}, k_i^{(1)}, k_i^{(2)})$ を短期秘密ストリング記憶部 2 1 0 に保存する。

[0073] S 2 0 1 - 2 2) ねじれ疑似ランダム関数部 2 0 3 は、 $m_i = \text{tPRF}_B(r_i^{(1)}, r_i^{(2)}, st_i, st'_i)$ と、 $n_i = \text{tPRF}_B(r_i^{(3)}, r_i^{(4)}, st_i, st'_i)$ と、 $k_i = \text{tPRF}(k_i^{(1)}, k_i^{(2)}, st_i, st'_i)$ とを生成する。なお、長期秘密ストリング (st_i, st'_i) は、長期秘密ストリング記憶部 2 0 9 は記憶されているものを使用する。

[0074] S 2 0 1 - 2 3) 同種写像計算部 2 0 4 は、 $[m_i]P_B + [n_i]Q_B$ で生成される E の部分群 K_i を核に持つ同種写像 $\phi_i: E \rightarrow E_i$ と、この同種写像 ϕ_i に付随する楕円曲線 E_i とを計算する。

[0075] S 2 0 1 - 2 4) 同種写像計算部 2 0 4 は、 $\phi_i(P_A)$ と $\phi_i(Q_A)$ とを計算する。

[0076] S 2 0 1 - 2 5) そして、通信部 2 0 8 は、 $(\phi_i(P_A), \phi_i(Q_A), E_i)$ を鍵配信サーバ 1 0 に送信する。これより、各ユーザ端末 2 0 $_i$ ($i = 2, 4, \dots, N$) の公開値 $(\phi_i(P_A), \phi_i(Q_A), E_i)$ が鍵配信サーバ 1 0 に送信される。

[0077] なお、上記のS 2 0 1 - 1 2 及びS 2 0 1 - 2 2 における m_i 及び n_i は、長期秘密ストリング記憶部2 0 9 に記憶されている長期秘密ストリングと、短期秘密ストリング記憶部2 1 0 に記憶されている短期秘密ストリングとを用いて、必要なときにねじれ疑似ランダム関数から生成することができる。このため、安全上、 m_i 及び n_i は保存しないことが好ましい。

[0078] ただし、安全性をあまり考慮しないのであれば、上記のS 2 0 1 - 1 2 で m_i 及び n_i を

[0079] [数18]

$$\mathbf{Z} / l_A^{e_A} \mathbf{Z}$$

からランダムに生成して、保存しておいても良い。同様に、上記のS 2 0 1 - 2 2 で m_i 及び n_i を

[0080] [数19]

$$\mathbf{Z} / l_B^{e_B} \mathbf{Z}$$

からランダムに生成して、保存しておいても良い。

[0081] ステップS 2 0 2 : 鍵配信ステップ (Round 1)

S 2 0 2 - 1) 通信部1 0 5 は、 i が奇数である各ユーザ端末2 0 $_i$ ($i = 1, 3, \dots, N-1$) から公開値 ($\phi_i(P_B)$, $\phi_i(Q_B)$, E_i) を受信すると共に、 i が偶数である各ユーザ端末2 0 $_i$ ($i = 2, 4, \dots, N$) から公開値 ($\phi_i(P_A)$, $\phi_i(Q_A)$, E_i) を受信する。

[0082] S 2 0 2 - 2) 通信部1 0 5 は、 i が奇数である各ユーザ端末2 0 $_i$ ($i = 1, 3, \dots, N-1$) に対して、(s_{id} , $\phi_{i-1}(P_A)$, $\phi_{i-1}(Q_A)$, E_{i-1} , $\phi_{i+1}(P_A)$, $\phi_{i+1}(Q_A)$, E_{i+1}) を送信する。

- [0083] また、通信部 105 は、 i が偶数である各ユーザ端末 20 _{i} ($i = 2, 4, \dots, N$) に対して、 $(sid, \phi_{i-1}(P_B), \phi_{i-1}(Q_B), E_{i-1}, \phi_{i+1}(P_B), \phi_{i+1}(Q_B), E_{i+1})$ を送信する。
- [0084] なお、上述したように、ユーザ端末 20 の添え字 i はリング状である。したがって、例えば、 $i = 1$ であるユーザ端末 20₁ に対しては、 $(sid, \phi_N(P_A), \phi_N(Q_A), E_N, \phi_2(P_A), \phi_2(Q_A), E_2)$ が送信される。また、例えば、 $i = N$ であるユーザ端末 20_N に対しては、 $(sid, \phi_{N-1}(P_B), \phi_{N-1}(Q_B), E_{N-1}, \phi_1(P_B), \phi_1(Q_B), E_1)$ が送信される。
- [0085] ステップ S203：第二鍵生成ステップ (Round 2)
以降の S203-11 ~ S203-16 は、 i が 1 以外の奇数である各ユーザ端末 20 _{i} ($i = 3, 5, \dots, N-1$) が実行する。
- [0086] S203-11) 通信部 208 は、鍵配信サーバ 10 から $(sid, \phi_{i-1}(P_A), \phi_{i-1}(Q_A), E_{i-1}, \phi_{i+1}(P_A), \phi_{i+1}(Q_A), E_{i+1})$ を受信する。
- [0087] S203-12) 同種写像計算部 204 は、 $[m_i] \phi_{i-1}(P_A) + [n_i] \phi_{i-1}(Q_A)$ で生成される E_{i-1} の部分群 $K_{i-1, i}$ を核に持つ同種写像 $\phi_{i-1, i} : E_{i-1} \rightarrow E_{i-1, i}$ と、この同種写像 $\phi_{i-1, i}$ に付随する楕円曲線 $E_{i-1, i}$ とを計算する。
- [0088] 同様に、同種写像計算部 204 は、 $[m_i] \phi_{i+1}(P_A) + [n_i] \phi_{i+1}(Q_A)$ で生成される E_{i+1} の部分群 $K_{i+1, i}$ を核に持つ同種写像 $\phi_{i+1, i} : E_{i+1} \rightarrow E_{i+1, i}$ と、この同種写像 $\phi_{i+1, i}$ に付随する楕円曲線 $E_{i+1, i}$ とを計算する。
- [0089] S203-13) 同種写像計算部 204 は、楕円曲線 $E_{i-1, i}$ の j 不変量 $j(E_{i-1, i})$ と、楕円曲線 $E_{i+1, i}$ の j 不変量 $j(E_{i+1, i})$ とを計算する。
- [0090] S203-14) 次に、第 1 疑似ランダム関数部 205 は、 $K_i^{(l)} = F(sid, j(E_{i-1, i}))$ と、 $K_i^{(r)} = F(sid, j(E_{i+1, i}))$ とを計算する。

[0091] S 2 0 3 - 1 5) 次に、第 1 疑似ランダム関数部 2 0 5 は、 $K_i^{(l)}$ と $K_i^{(r)}$ とのビット毎の排他的論理和 T_i を計算する。すなわち、第 1 疑似ランダム関数部 2 0 5 は、

[0092] [数20]

$$T_i = K_i^{(l)} \oplus K_i^{(r)}$$

ここで、 $\oplus$ は排他的論理和を表す

を計算する。

[0093] S 2 0 3 - 1 6) そして、通信部 2 0 8 は、 (k_i, T_i) を鍵配信サーバ 1 0 に送信する。なお、 k_i は、第一鍵生成ステップ (S 2 0 1) で生成されたものである。

[0094] 以降の S 2 0 3 - 2 1 ~ S 2 0 3 - 2 6 は、 i が偶数である各ユーザ端末 2 0 i ($i = 2, 4, \dots, N$) が実行する。

[0095] S 2 0 3 - 2 1) 通信部 2 0 8 は、鍵配信サーバ 1 0 から $(sid, \phi_{i-1}(P_B), \phi_{i-1}(Q_B), E_{i-1}, \phi_{i+1}(P_B), \phi_{i+1}(Q_B), E_{i+1})$ を受信する。

[0096] S 2 0 3 - 2 2) 同種写像計算部 2 0 4 は、 $[m_i] \phi_{i-1}(P_B) + [n_i] \phi_{i-1}(Q_B)$ で生成される E_{i-1} の部分群 $K_{i-1,i}$ を核に持つ同種写像 $\phi_{i-1,i} : E_{i-1} \rightarrow E_{i-1,i}$ と、この同種写像 $\phi_{i-1,i}$ に付随する楕円曲線 $E_{i-1,i}$ とを計算する。

[0097] 同様に、同種写像計算部 2 0 4 は、 $[m_i] \phi_{i+1}(P_B) + [n_i] \phi_{i+1}(Q_B)$ で生成される E_{i+1} の部分群 $K_{i+1,i}$ を核に持つ同種写像 $\phi_{i+1,i} : E_{i+1} \rightarrow E_{i+1,i}$ と、この同種写像 $\phi_{i+1,i}$ に付随する楕円曲線 $E_{i+1,i}$ とを計算する。

[0098] S 2 0 3 - 2 3) 同種写像計算部 2 0 4 は、楕円曲線 $E_{i-1,i}$ の j 不変量 $j(E_{i-1,i})$ と、楕円曲線 $E_{i+1,i}$ の j 不変量 $j(E_{i+1,i})$ とを計算する。

- [0099] S 2 0 3 - 2 4) 次に、第 1 疑似ランダム関数部 2 0 5 は、 $K_i^{(l)} = F(sid, j(E_{i-1}, i))$ と、 $K_i^{(r)} = F(sid, j(E_{i+1}, i))$ とを計算する。
- [0100] S 2 0 3 - 2 5) 次に、第 1 疑似ランダム関数部 2 0 5 は、 $K_i^{(l)}$ と $K_i^{(r)}$ とのビット毎の排他的論理和 T_i を計算する。
- [0101] S 2 0 3 - 2 6) そして、通信部 2 0 8 は、 (k_i, T_i) を鍵配信サーバ 1 0 に送信する。なお、 k_i は、第一鍵生成ステップ (S 2 0 1) で生成されたものである。
- [0102] 以降の S 2 0 3 - 3 1 ~ S 2 0 3 - 3 7 は、代表ユーザ端末であるユーザ端末 2 0 1 が実行する。
- [0103] S 2 0 3 - 3 1) 通信部 2 0 8 は、鍵配信サーバ 1 0 から $(sid, \phi_N(P_A), \phi_N(Q_A), E_N, \phi_2(P_A), \phi_2(Q_A), E_2)$ を受信する。
- [0104] S 2 0 3 - 3 2) 同種写像計算部 2 0 4 は、 $[m_1] \phi_N(P_A) + [n_1] \phi_N(Q_A)$ で生成される E_N の部分群 $K_{N,1}$ を核に持つ同種写像 $\phi_{N,1} : E_N \rightarrow E_{N,1}$ と、この同種写像 $\phi_{N,1}$ に付随する楕円曲線 $E_{N,1}$ とを計算する。
- [0105] 同様に、同種写像計算部 2 0 4 は、 $[m_1] \phi_2(P_A) + [n_1] \phi_2(Q_A)$ で生成される E_2 の部分群 $K_{2,1}$ を核に持つ同種写像 $\phi_{2,1} : E_2 \rightarrow E_{2,1}$ と、この同種写像 $\phi_{2,1}$ に付随する楕円曲線 $E_{2,1}$ とを計算する。
- [0106] S 2 0 3 - 3 3) 同種写像計算部 2 0 4 は、楕円曲線 $E_{N,1}$ の j 不変量 $j(E_{N,1})$ と、楕円曲線 $E_{2,1}$ の j 不変量 $j(E_{2,1})$ とを計算する。
- [0107] S 2 0 3 - 3 4) 次に、第 1 疑似ランダム関数部 2 0 5 は、 $K_1^{(l)} = F(sid, j(E_{N,1}))$ と、 $K_1^{(r)} = F(sid, j(E_{2,1}))$ とを計算する。
- [0108] S 2 0 3 - 3 5) 次に、第 1 疑似ランダム関数部 2 0 5 は、 $K_1^{(l)}$ と $K_1^{(r)}$ とのビット毎の排他的論理和 T_1 を計算する。
- [0109] S 2 0 3 - 3 6) 次に、第 1 疑似ランダム関数部 2 0 5 は、 $K_1^{(l)}$ と k_1 との排他的論理和 T' を計算する。すなわち、第 1 疑似ランダム関数部 2 0 5 は、

[0110] [数21]

$$T' = K_1^{(l)} \oplus k_1$$

を計算する。なお、 k_1 は、第一鍵生成ステップ（S201）で生成されたものである。

[0111] S203-37) そして、通信部208は、 (T', T_1) を鍵配信サーバ10に送信する。

[0112] ステップS204：第三鍵生成ステップ（Round2）

S204-1) 通信部105は、 $i=1$ であるユーザ端末20₁から (T', T_1) を受信すると共に、 i が1以外の各ユーザ端末20_{*i*}（ $i=2, 3, \dots, N$ ）から (k_i, T_i) を受信する。

[0113] S204-2) 短期秘密ストリング生成部103は、短期秘密ストリングとして、 $k_s^{(1)} \in \{0, 1\}^k$ と、 $k_s^{(2)} \in \text{Kspace}_k$ とを一様ランダムに生成する。そして、短期秘密ストリング生成部103は、短期秘密ストリング $(k_s^{(1)}, k_s^{(2)})$ を短期秘密ストリング記憶部107に保存する。

[0114] S204-3) 次に、短期秘密ストリング生成部103は、短期秘密ストリング生成部103は、 $k_s = \text{tPRF}(k_s^{(1)}, k_s^{(2)}, st_s, st'_s)$ と、

[0115] [数22]

$$k' = (\oplus_{2 \leq i \leq N} k_i) \oplus k_s$$

とを計算する。なお、 st_s 及び st'_s は、長期秘密ストリング記憶部106に保存されているものを使用する。

[0116] S204-4) 次に、公開情報計算部104は、各 $i \in \{2, \dots, N$

に対して、各 T_j ($1 \leq j \leq i-1$) 同士の排他的論理和 T'_i を計算する。
すなわち、公開情報計算部 104 は、

[0117] [数23]

$$T'_i = \bigoplus_{1 \leq j \leq i-1} T_j$$

を計算する。

[0118] S204-5) そして、通信部 105 は、各ユーザ端末 20_i ($i = 2, \dots, N$) に対して、(k' , T'_i , T') を送信する。また、通信部 105 は、ユーザ端末 20₁ に対して、 k' を送信する。

[0119] ステップ S205 : セッション鍵生成ステップ

以降の S205-11 ~ S205-14 は、 i が 1 以外であるユーザ端末 20_i (すなわち、代表ユーザ端末以外のユーザ端末 20) が実行する。

[0120] S205-11) 通信部 208 は、鍵配信サーバ 10 から (k' , T'_i , T') を受信する。

[0121] S205-12) 秘密情報計算部 206 は、 T'_i と T' との排他的論理和を計算する。この排他的論理和は $K_1^{(i)}$ と一致する。すなわち、

[0122] [数24]

$$K_1^{(i)} = T'_i \oplus T'$$

である。

[0123] S205-13) 次に、秘密情報計算部 206 は、 T' と $K_1^{(i)}$ との排他的論理和を計算する。この排他的論理和は k_1 と一致する。すなわち、

[0124]

[数25]

$$k_1 = T' \oplus K_1^{(l)}$$

である。

[0125] S 2 0 5 - 1 4) 次に、第2疑似ランダム関数部 2 0 7 は、

[0126] [数26]

$$K = F'(sid, k' \oplus k_1)$$

を計算する。このKがセッション鍵となる。

[0127] そして、第2疑似ランダム関数部 2 0 7 は、セッション鍵Kをセッション情報記憶部 2 1 1 に保存する。

[0128] 以降の S 2 0 5 - 2 1 ~ S 2 0 5 - 2 2 は、i が1であるユーザ端末 2 0 , (すなわち、代表ユーザ端末) が実行する。

[0129] S 2 0 5 - 2 1) 通信部 2 0 8 は、鍵配信サーバ 1 0 から k ' を受信する。
。

[0130] S 2 0 5 - 2 2) 次に、第2疑似ランダム関数部 2 0 7 は、

[0131] [数27]

$$K = F'(sid, k' \oplus k_1)$$

を計算する。このKがセッション鍵となる。

[0132] そして、第2疑似ランダム関数部 2 0 7 は、セッション鍵Kをセッション情報記憶部 2 1 1 に保存する。

[0133] これにより、各ユーザ端末 20_i ($i = 1, 2, \dots, N$) 間で同一のセッション鍵 K が共有される。このセッション鍵 K を用いて、各ユーザ端末 20 間で送受信されるデータが暗号化される。

[0134] ≪ N が奇数である場合 ≫

次に、 N が奇数である場合について説明する。なお、 N が偶数である場合に説明した処理と同様の処理を行う箇所については、適宜、その説明を省略又は簡略化する。

[0135] ステップ $S201$: 第一鍵生成ステップ (Round 1)

i が 1 以外の奇数である各ユーザ端末 20_i ($i = 3, 5, \dots, N$) は、上記の $S201-11 \sim S201-15$ を実行する。また、 i が偶数である各ユーザ端末 20_i ($i = 2, 4, \dots, N-1$) は、上記の $S201-21 \sim S201-25$ を実行する。

[0136] 以降の $S201-31 \sim S201-35$ は、 i が 1 であるユーザ端末 20_1 (すなわち、代表ユーザ端末) が実行する。

[0137] $S201-31$) 短期秘密ストリング生成部 202 は、短期秘密ストリングとして、 $r_1^{(1)} \in \{0, 1\}^k$ と、 $r_1^{(2)} \in \text{Kspace}_k$ と、 $r_1^{(3)} \in \{0, 1\}^k$ と、 $r_1^{(4)} \in \text{Kspace}_k$ と、 $r_1^{(5)} \in \{0, 1\}^k$ と、 $r_1^{(6)} \in \text{Kspace}_k$ と、 $r_1^{(7)} \in \{0, 1\}^k$ と、 $r_1^{(8)} \in \text{Kspace}_k$ と、 $k_1^{(1)} \in \{0, 1\}^k$ と、 $k_1^{(2)} \in \text{Kspace}_k$ とを一様ランダムに生成する。

[0138] そして、短期秘密ストリング生成部 202 は、短期秘密ストリング ($r_1^{(1)}$, $r_1^{(2)}$, $r_1^{(3)}$, $r_1^{(4)}$, $r_1^{(5)}$, $r_1^{(6)}$, $r_1^{(7)}$, $r_1^{(8)}$, $k_1^{(1)}$, $k_2^{(2)}$) を短期秘密ストリング記憶部 210 に保存する。

[0139] $S201-32$) ねじれ疑似ランダム関数部 203 は、 $m_1 = \text{tPRF}_A(r_1^{(1)}, r_1^{(2)}, st_1, st'_1)$ と、 $n_1 = \text{tPRF}_A(r_1^{(3)}, r_1^{(4)}, st_1, st'_1)$ と、 $m_{N+1} = \text{tPRF}_B(r_1^{(5)}, r_1^{(6)}, st_1, st'_1)$ と、 $n_{N+1} = \text{tPRF}_B(r_1^{(7)}, r_1^{(8)}, st_1, st'_1)$ と、 $k_1 = \text{tPRF}(k_1^{(1)}, k_1^{(2)}, st_1, st'_1)$ とを生成する。なお、長期

秘密ストリング ($s t_1, s t'_1$) は、長期秘密ストリング記憶部 209 は記憶されているものを使用する。

[0140] S 201-33) 同種写像計算部 204 は、 $[m_1] P_A + [n_1] Q_A$ で生成される E の部分群 K_1 を核に持つ同種写像 $\phi_1: E \rightarrow E_1$ と、この同種写像 ϕ_1 に付随する楕円曲線 E_1 とを計算する。

[0141] また、同種写像計算部 204 は、 $[m_{N+1}] P_B + [n_{N+1}] Q_B$ で生成される E の部分群 K_{N+1} を核に持つ同種写像 $\phi_{N+1}: E \rightarrow E_{N+1}$ と、この同種写像 ϕ_{N+1} に付随する楕円曲線 E_{N+1} とを計算する。

[0142] S 201-34) 同種写像計算部 204 は、 $\phi_1(P_B)$ と、 $\phi_1(Q_B)$ と、 $\phi_{N+1}(P_A)$ と、 $\phi_{N+1}(Q_A)$ とを計算する。

[0143] S 201-35) そして、通信部 208 は、 $(\phi_1(P_B), \phi_1(Q_B), E_1, \phi_{N+1}(P_A), \phi_{N+1}(Q_B), E_{N+1})$ を鍵配信サーバ 10 に送信する。これより、代表ユーザ端末であるユーザ端末 201 の公開値 $(\phi_1(P_B), \phi_1(Q_B), E_1, \phi_{N+1}(P_A), \phi_{N+1}(Q_B), E_{N+1})$ が鍵配信サーバ 10 に送信される。

[0144] なお、上記の S 201-32) における m_1, n_1, m_{N+1} 及び n_{N+1} は、長期秘密ストリング記憶部 209 に記憶されている長期秘密ストリングと、短期秘密ストリング記憶部 210 に記憶されている短期秘密ストリングとを用いて、必要なときにねじれ疑似ランダム関数から生成することができる。このため、安全上、 m_1, n_1, m_{N+1} 及び n_{N+1} は保存しないことが好ましい。

[0145] ただし、安全性をあまり考慮しないのであれば、上記の S 201-32) で m_1 及び n_1 を

[0146] [数 28]

$$\mathbb{Z} / l_A^e \mathbb{Z}$$

からランダムに生成すると共に、 m_{N+1} 及び n_{N+1} を

[0147] [数29]

$$\mathbf{Z} / l_B^{e_B} \mathbf{Z}$$

からランダムに生成し、保存しておいても良い。

[0148] ステップS202：鍵配信ステップ (Round 1)

S202-3) 通信部105は、 i が1であるユーザ端末20₁から公開値 ($\phi_1(P_B)$, $\phi_1(Q_B)$, E_1 , $\phi_{N+1}(P_A)$, $\phi_{N+1}(Q_B)$, E_{N+1})を受信する。また、通信部105は、 i が1以外の奇数である各ユーザ端末20 _{i} ($i=3, 5, \dots, N$)から公開値 ($\phi_i(P_B)$, $\phi_i(Q_B)$, E_i)を受信すると共に、 i が偶数である各ユーザ端末20 _{i} ($i=2, 4, \dots, N-1$)から公開値 ($\phi_i(P_A)$, $\phi_i(Q_A)$, E_i)を受信する。

[0149] S202-4) 通信部105は、 i が奇数である各ユーザ端末20 _{i} ($i=1, 3, \dots, N$)に対して、($s i d$, $\phi_{i-1}(P_A)$, $\phi_{i-1}(Q_A)$, E_{i-1} , $\phi_{i+1}(P_A)$, $\phi_{i+1}(Q_A)$, E_{i+1})を送信する。

[0150] また、通信部105は、 i が偶数である各ユーザ端末20 _{i} ($i=2, 4, \dots, N-1$)に対して、($s i d$, $\phi_{i-1}(P_B)$, $\phi_{i-1}(Q_B)$, E_{i-1} , $\phi_{i+1}(P_B)$, $\phi_{i+1}(Q_B)$, E_{i+1})を送信する。

[0151] ステップS203：第二鍵生成ステップ (Round 2)

i が1以外の奇数である各ユーザ端末20 _{i} ($i=3, 5, \dots, N$)は、上記のS203-11~S203-16を実行する。また、 i が偶数である各ユーザ端末20 _{i} ($i=2, 4, \dots, N-1$)は、上記のS203-21~S203-26を実行する。

[0152] 以降のS203-41~S203-47は、 i が1であるユーザ端末20₁ (すなわち、代表ユーザ端末)が実行する。

[0153] S203-41) 通信部208は、鍵配信サーバ10から ($s i d$, $\phi_N(P_A)$, $\phi_N(Q_A)$, E_N , $\phi_2(P_A)$, $\phi_2(Q_A)$, E_2)を受信する。

[0154] S 2 0 3 - 4 2) 同種写像計算部 2 0 4 は、 $[m_{N+1}] \phi_N(P_B) + [n_{N+1}] \phi_N(Q_B)$ で生成される E_N の部分群 $K_{N, N+1}$ を核に持つ同種写像 $\phi_{N, N+1} : E_N \rightarrow E_{N, N+1}$ と、この同種写像 $\phi_{N, N+1}$ に付随する楕円曲線 $E_{N, N+1}$ とを計算する。

[0155] 同様に、同種写像計算部 2 0 4 は、 $[m_1] \phi_2(P_A) + [n_1] \phi_2(Q_A)$ で生成される E_2 の部分群 $K_{2, 1}$ を核に持つ同種写像 $\phi_{2, 1} : E_2 \rightarrow E_{2, 1}$ と、この同種写像 $\phi_{2, 1}$ に付随する楕円曲線 $E_{2, 1}$ とを計算する。

[0156] S 2 0 3 - 4 3) 同種写像計算部 2 0 4 は、楕円曲線 $E_{N, N+1}$ の j 不変量 $j(E_{N, N+1})$ と、楕円曲線 $E_{2, 1}$ の j 不変量 $j(E_{2, 1})$ とを計算する。

[0157] S 2 0 3 - 4 4) 次に、第 1 疑似ランダム関数部 2 0 5 は、 $K_1^{(l)} = F(sid, j(E_{N, N+1}))$ と、 $K_1^{(r)} = F(sid, j(E_{2, 1}))$ とを計算する。

[0158] S 2 0 3 - 4 5) 次に、第 1 疑似ランダム関数部 2 0 5 は、 $K_1^{(l)}$ と $K_1^{(r)}$ とのビット毎の排他的論理和 T_1 を計算する。

[0159] S 2 0 3 - 4 6) 次に、第 1 疑似ランダム関数部 2 0 5 は、 $K_1^{(l)}$ と k_1 との排他的論理和 T' を計算する。

[0160] S 2 0 3 - 4 7) そして、通信部 2 0 8 は、 (T', T_1) を鍵配信サーバ 1 0 に送信する。

[0161] 以降のステップ S 2 0 4 ~ ステップ S 2 0 5 は、 N が偶数である場合と同様であるため、その説明を省略する。

[0162] (実施例 2)

以降では、実施例 2 について説明する。実施例 2 は、 N が偶数又は奇数のいずれであっても同様の処理を行うものである。すなわち、実施例 2 では、実施例 1 と異なり、 N の偶奇による場合分けが発生しない。

[0163] ステップ S 2 0 1 : 第一鍵生成ステップ (Round 1)

以降の S 2 0 1 - 4 1 ~ S 2 0 1 - 4 5 は、各ユーザ端末 2 0 $_i$ ($i = 1, 2, \dots, N$) が実行する。

[0164] S 2 0 1 - 4 1) 短期秘密ストリング生成部 2 0 2 は、短期秘密ストリン

グとして、 $r_i^{(1)} \in \{0, 1\}^k$ と、 $r_i^{(2)} \in \text{Kspace}_k$ と、 $r_i^{(3)} \in \{0, 1\}^k$ と、 $r_i^{(4)} \in \text{Kspace}_k$ と、 $r_i^{(5)} \in \{0, 1\}^k$ と、 $r_i^{(6)} \in \text{Kspace}_k$ と、 $r_i^{(7)} \in \{0, 1\}^k$ と、 $r_i^{(8)} \in \text{Kspace}_k$ と、 $k_i^{(1)} \in \{0, 1\}^k$ と、 $k_i^{(2)} \in \text{Kspace}_k$ とを一様ランダムに生成する。

[0165] そして、短期秘密ストリング生成部202は、短期秘密ストリング($r_i^{(1)}$, $r_i^{(2)}$, $r_i^{(3)}$, $r_i^{(4)}$, $r_i^{(5)}$, $r_i^{(6)}$, $r_i^{(7)}$, $r_i^{(8)}$, $k_i^{(1)}$, $k_i^{(2)}$)を短期秘密ストリング記憶部210に保存する。

[0166] S201-42)ねじれ疑似ランダム関数部203は、 $m_i^{(1)} = \text{tPRF}_A(r_i^{(1)}, r_i^{(2)}, st_i, st'_i)$ と、 $n_i^{(1)} = \text{tPRF}_A(r_i^{(3)}, r_i^{(4)}, st_i, st'_i)$ と、 $m_i^{(2)} = \text{tPRF}_B(r_i^{(5)}, r_i^{(6)}, st_i, st'_i)$ と、 $n_i^{(2)} = \text{tPRF}_B(r_i^{(7)}, r_i^{(8)}, st_i, st'_i)$ と、 $k_i = \text{tPRF}(k_i^{(1)}, k_i^{(2)}, st_i, st'_i)$ とを生成する。なお、長期秘密ストリング(st_i, st'_i)は、長期秘密ストリング記憶部209は記憶されているものを使用する。

[0167] S201-43)同種写像計算部204は、 $[m_i^{(1)}]P_A + [n_i^{(1)}]Q_A$ で生成されるEの部分群 $K_i^{(1)}$ を核に持つ同種写像 $\phi_i^{(1)}: E \rightarrow E_i^{(1)}$ と、この同種写像 $\phi_i^{(1)}$ に付随する楕円曲線 $E_i^{(1)}$ とを計算する。

[0168] また、同種写像計算部204は、 $[m_i^{(2)}]P_B + [n_i^{(2)}]Q_B$ で生成されるEの部分群 $K_i^{(2)}$ を核に持つ同種写像 $\phi_i^{(2)}: E \rightarrow E_i^{(2)}$ と、この同種写像 $\phi_i^{(2)}$ に付随する楕円曲線 $E_i^{(2)}$ とを計算する。

[0169] S201-44)同種写像計算部204は、 $\phi_i^{(1)}(P_B)$ と、 $\phi_i^{(1)}(Q_B)$ と、 $\phi_i^{(2)}(P_A)$ と、 $\phi_i^{(2)}(Q_A)$ とを計算する。

[0170] S201-45)そして、通信部208は、($\phi_i^{(1)}(P_B)$, $\phi_i^{(1)}(Q_B)$, $E_i^{(1)}$, $\phi_i^{(2)}(P_A)$, $\phi_i^{(2)}(Q_B)$, $E_i^{(2)}$)を鍵配信サーバ10に送信する。これより、各ユーザ端末20_iの公開値($\phi_i^{(1)}(P_B)$, $\phi_i^{(1)}(Q_B)$, $E_i^{(1)}$, $\phi_i^{(2)}(P_A)$, $\phi_i^{(2)}(Q_B)$, $E_i^{(2)}$)が鍵配信サーバ10に送信される。

[0171] なお、上記の S 2 0 1 - 4 2 における $m_i^{(1)}$, $n_i^{(1)}$, $m_i^{(2)}$ 及び $n_i^{(2)}$ は、長期秘密ストリング記憶部 2 0 9 に記憶されている長期秘密ストリングと、短期秘密ストリング記憶部 2 1 0 に記憶されている短期秘密ストリングとを用いて、必要なときにねじれ疑似ランダム関数から生成することができる。このため、安全上、 $m_i^{(1)}$, $n_i^{(1)}$, $m_i^{(2)}$ 及び $n_i^{(2)}$ は保存しないことが好ましい。

[0172] ただし、安全性をあまり考慮しないのであれば、上記の S 2 0 1 - 3 2 で $m_i^{(1)}$ 及び $n_i^{(1)}$ を

[0173] [数30]

$$\mathbf{Z} / l_A^{e_A} \mathbf{Z}$$

からランダムに生成すると共に、 $m_i^{(2)}$ 及び $n_i^{(2)}$ を

[0174] [数31]

$$\mathbf{Z} / l_B^{e_B} \mathbf{Z}$$

からランダムに生成し、保存しておいても良い。

[0175] ステップ S 2 0 2 : 鍵配信ステップ (Round 1)

S 2 0 2 - 5) 通信部 1 0 5 は、各ユーザ端末 2 0 i から公開値 ($\phi_i^{(1)}$ (P_B), $\phi_i^{(1)}$ (Q_B), $E_i^{(1)}$, $\phi_i^{(2)}$ (P_A), $\phi_i^{(2)}$ (Q_B), $E_i^{(2)}$) を受信する。

[0176] S 2 0 2 - 6) 通信部 1 0 5 は、各ユーザ端末 2 0 i に対して、(s_{id} , $\phi_{i-1}^{(1)}$ (P_B), $\phi_{i-1}^{(1)}$ (Q_B), $E_{i-1}^{(1)}$, $\phi_{i+1}^{(2)}$ (P_A), $\phi_{i+1}^{(2)}$ (Q_B), $E_{i+1}^{(2)}$) を送信する。

[0177] ステップ S 2 0 3 : 第二鍵生成ステップ (Round 2)

以降のS201-51~S201-56は、各ユーザ端末20_i ($i = 1, 2, \dots, N$) が実行する。ただし、S201-54~S203-56は、代表ユーザ端末であるユーザ端末20₁と、それ以外のユーザ端末20_i ($i = 2, 3, \dots, N$) とで処理内容が異なる。

[0178] S203-51) 通信部208は、鍵配信サーバ10から ($s i d, \phi_{i-1}^{(1)} (P_B), \phi_{i-1}^{(1)} (Q_B), E_{i-1}^{(1)}, \phi_{i+1}^{(2)} (P_A), \phi_{i+1}^{(2)} (Q_B), E_{i+1}^{(2)}$) を受信する。

[0179] S203-52) 同種写像計算部204は、 $[m_i^{(2)}] \phi_{i-1}^{(1)} (P_B) + [n_i^{(2)}] \phi_{i-1}^{(1)} (Q_B)$ で生成される $E_{i-1}^{(1)}$ の部分群 $K_{i-1, i}^{(1)}$ を核に持つ同種写像 $\phi_{i-1, i}^{(1)} : E_{i-1}^{(1)} \rightarrow E_{i-1, i}^{(1)}$ と、この同種写像 $\phi_{i-1, i}^{(1)}$ に付随する楕円曲線 $E_{i-1, i}^{(1)}$ とを計算する。

[0180] 同様に、同種写像計算部204は、 $[m_i^{(1)}] \phi_{i+1}^{(2)} (P_A) + [n_i^{(1)}] \phi_{i+1}^{(2)} (Q_A)$ で生成される $E_{i+1}^{(2)}$ の部分群 $K_{i+1, i}^{(2)}$ を核に持つ同種写像 $\phi_{i+1, i}^{(2)} : E_{i+1}^{(2)} \rightarrow E_{i+1, i}^{(2)}$ と、この同種写像 $\phi_{i+1, i}^{(2)}$ に付随する楕円曲線 $E_{i+1, i}^{(2)}$ とを計算する。

[0181] S203-53) 同種写像計算部204は、楕円曲線 $E_{i-1, i}^{(1)}$ の j 不変量 $j(E_{i-1, i}^{(1)})$ と、楕円曲線 $E_{i+1, i}^{(2)}$ の j 不変量 $j(E_{i+1, i}^{(2)})$ とを計算する。

[0182] S203-54) ユーザ端末20_i ($i = 2, 3, \dots, N$) の第1疑似ランダム関数部205は、 $K_i^{(1)} = F(s i d, j(E_{i-1, i}^{(1)}))$ と、 $K_i^{(r)} = F(s i d, j(E_{i+1, i}^{(2)}))$ とを計算する。

[0183] また、ユーザ端末20₁の第1疑似ランダム関数部205は、 $K_1^{(1)} = F(s i d, j(E_{N, 1}^{(1)}))$ と、 $K_1^{(r)} = F(s i d, j(E_{2, 1}^{(2)}))$ とを計算する。

[0184] S203-55) 次に、ユーザ端末20_i ($i = 2, 3, \dots, N$) の第1疑似ランダム関数部205は、 $K_i^{(1)}$ と $K_i^{(r)}$ とのビット毎の排他的論理和 T_i を計算する。

[0185] また、ユーザ端末20₁の第1疑似ランダム関数部205は、 $K_1^{(1)}$ と K_1

(r)との排他的論理和 T_1 を計算すると共に、 $K_1^{(1)}$ と k_1 との排他的論理和 T' を計算する。なお、 k_1 は、第一鍵生成ステップ(S201)で生成されたものである。

[0186] S203-56)そして、ユーザ端末20_i($i=2, 3, \dots, N$)の通信部208は、(k_i, T_i)を鍵配信サーバ10に送信する。なお、 k_i は、第一鍵生成ステップ(S201)で生成されたものである。

[0187] また、ユーザ端末20₁の通信部208は、(T', T_1)を鍵配信サーバ10に送信する。

[0188] 以降のステップS204～ステップS205は、実施例1と同様であるため、その説明を省略する。

[0189] <ハードウェア構成>

図6に示すように、本発明の実施の形態における鍵配信サーバ10及びユーザ端末20は、入力装置301と、表示装置302と、外部I/F303と、RAM(Random Access Memory)304と、ROM(Read Only Memory)305と、CPU(Central Processing Unit)306と、通信I/F307と、補助記憶装置308とを有する。これら各ハードウェアは、それぞれがバスBを介して通信可能に接続されている。

[0190] 入力装置301は、例えばキーボードやマウス、タッチパネル等である。表示装置302は、例えばディスプレイ等である。なお、鍵配信サーバ10は、入力装置301及び表示装置302のうちの少なくとも一方を有していても良い。

[0191] 外部I/F303は、外部装置とのインタフェースである。外部装置には、記録媒体303a等がある。記録媒体303aとしては、例えば、CD(Compact Disc)、DVD(Digital Versatile Disk)、SDメモリカード(Secure Digital memory card)、USB(Universal Serial Bus)メモリカード等が挙げられる。記録媒体303aには、鍵配信サーバ10の各機能部を実現する1以上のプログラムやユーザ端末20の各機能部を実現する1以上のプログラム等が記録されていても良い。

[0192] RAM 304 は、プログラムやデータを一時保持する揮発性の半導体メモリである。ROM 305 は、電源を切ってもプログラムやデータを保持することができる不揮発性の半導体メモリである。

[0193] CPU 306 は、ROM 305 や補助記憶装置 308 等からプログラムやデータを RAM 304 上に読み出して処理を実行する演算装置である。鍵配信サーバ 10 の各機能部やユーザ端末 20 の各機能部は、CPU 306 が 1 以上のプログラムを実行することによって実現される。

[0194] 通信 I/F 307 は、ネットワーク 30 に接続するためのインタフェースである。なお、鍵配信サーバ 10 の各機能部を実現する 1 以上のプログラムやユーザ端末 20 の各機能部を実現する 1 以上のプログラム等は、通信 I/F 307 を介して、所定のサーバ等から取得（ダウンロード）されても良い。

[0195] 補助記憶装置 308 は、例えば HDD（Hard Disk Drive）や SSD（Solid State Drive）等の不揮発性の記憶装置である。補助記憶装置 308 には、鍵配信サーバ 10 の各機能部を実現する 1 以上のプログラムやユーザ端末 20 の各機能部を実現する 1 以上のプログラム等が記録される。

[0196] 本発明の実施の形態における鍵配信サーバ 10 及びユーザ端末 20 は、図 6 に示すハードウェア構成を有することにより、上述した各種処理を実現することができる。なお、図 6 では、本発明の実施の形態における鍵配信サーバ 10 が 1 台の情報処理装置で実現される場合を示したが、これに限られない。本発明の実施の形態における鍵配信サーバ 10 は、複数台の情報処理装置で実現されていても良い。

[0197] <まとめ>

以上のように、本発明の実施の形態における鍵交換システム 1 では、DMKD プロトコルにおける DH 鍵交換を同種写像暗号に変更することで、耐量子性がある多者間鍵交換を実現することができる。

[0198] しかも、本発明の実施の形態における鍵交換システム 1 の実施例 1 では、ユーザ端末 20 の台数 N が偶数である場合、例えば、ユーザ端末 20₁、ユー

ザ端末 20_3 , $\dots$, ユーザ端末 20_{N-1} が基底 $\{P_A, Q_A\}$ からそれぞれ公開値を計算し、ユーザ端末 20_2 , ユーザ端末 20_4 , $\dots$, ユーザ端末 20_N が基底 $\{P_B, Q_B\}$ からそれぞれ公開値を計算する。これにより、(論理的に) リング状に配置されるユーザ端末 20 の隣り合うユーザ端末 20 同士は、異なる基底を使用して公開値を計算することになり、隣り合うユーザ端末 20 同士での同種写像暗号の鍵交換を少ないラウンド数(2ラウンド)で容易に行うことができるようになる。

[0199] 一方で、ユーザ端末 20 の台数 N が奇数である場合、代表ユーザ端末であるユーザ端末 20_1 が基底 $\{P_A, Q_A\}$ 及び基底 $\{P_B, Q_B\}$ の両方からそれぞれ公開値を計算し、ユーザ端末 20_3 , ユーザ端末 20_5 , $\dots$, ユーザ端末 20_{N-1} が基底 $\{P_A, Q_A\}$ からそれぞれ公開値を計算し、ユーザ端末 20_2 , ユーザ端末 20_4 , $\dots$, ユーザ端末 20_N が基底 $\{P_B, Q_B\}$ からそれぞれ公開値を計算する。このように、代表ユーザ端末が両方の基底 $\{P_A, Q_A\}$ 及び $\{P_B, Q_B\}$ からそれぞれ公開値を計算することで、ユーザ端末 20 全体として、 N が偶数である場合と同様の振る舞いを実現することができ、同種写像暗号の鍵交換を少ないラウンド数で容易に行うことができるようになる。

[0200] また、本発明の実施の形態における鍵交換システム 1 の実施例 2 では、ユーザ端末 20 の台数 N の偶奇によらず、全てのユーザ端末 20 が基底 $\{P_A, Q_A\}$ 及び基底 $\{P_B, Q_B\}$ の両方からそれぞれ公開値を計算する。これにより、ユーザ端末 20 全体として、実施例 1 の N が偶数である場合と同様の振る舞いを実現することができ、同種写像暗号の鍵交換を少ないラウンド数で容易に行うことができるようになる。更に、実施例 2 では、ユーザ数の偶奇に関わらず、同一の処理内容を用いるため、例えば、ユーザの偶奇に応じて条件分岐等が発生しない鍵交換処理を実現することができる。

[0201] このように、本発明の実施の形態における鍵交換システム 1 では、耐量子性があり、かつ、非特許文献 1 と比べて少ないラウンド数(2ラウンド)の多者間鍵交換(すなわち、耐量子性があり、かつ、通信コストが少ない多者

間鍵交換)を実現することができる。

[0202] 本発明は、具体的に開示された上記の実施形態に限定されるものではなく、特許請求の範囲から逸脱することなく、種々の変形や変更が可能である。

[0203] 本願は、日本国に2018年4月11日出願された基礎出願2018-076343号に基づくものであり、その全内容はここに参照をもって援用される。

符号の説明

[0204]	1	鍵交換システム
	10	鍵配信サーバ
	20	ユーザ端末
	101	セットアップ部
	102	長期秘密ストリング生成部
	103	短期秘密ストリング生成部
	104	公開情報計算部
	105	通信部
	106	長期秘密ストリング記憶部
	107	短期秘密ストリング記憶部
	201	長期秘密ストリング生成部
	202	短期秘密ストリング生成部
	203	ねじれ疑似ランダム関数部
	204	同種写像計算部
	205	第1疑似ランダム関数部
	206	秘密情報計算部
	207	第2疑似ランダム関数部
	208	通信部
	209	長期秘密ストリング記憶部
	210	短期秘密ストリング記憶部
	211	セッション情報記憶部

請求の範囲

[請求項1]

N (ただし、 $N \geq 2$) 台の端末装置 U_i ($i = 1, \dots, N$) と、該 N 台の端末装置 U_i 間で同種写像暗号によるセッション鍵の交換に用いられる鍵配信サーバとが含まれる鍵配信システムであって、

N が偶数である場合、前記端末装置 U_i のうち、奇数番目の端末装置 U_i ($i = 1, \dots, N-1$) が所定の楕円曲線の第1のねじれ部分群の基底を用いた第1の公開値を計算し、偶数番目の端末装置 U_i ($i = 2, \dots, N$) が前記楕円曲線の第2のねじれ部分群の基底を用いた第2の公開値を計算する同種写像計算手段と、

前記鍵配信サーバが、奇数番目の端末装置 U_i により計算された第1の公開値を端末装置 U_{i-1} (ただし、 $i = 1$ である場合、 $U_0 = U_N$) 及び端末装置 U_{i+1} (ただし、 $i = N$ である場合、 $U_{N+1} = U_1$) に配信し、偶数番目の端末装置 U_i により計算された第2の公開値を端末装置 U_{i-1} 及び端末装置 U_{i+1} に配信する配信手段と、

前記配信手段により配信された第2の公開値を用いて奇数番目の端末装置 U_i が前記セッション鍵を生成し、前記配信手段により配信された第1の公開値を用いて偶数番目の端末装置 U_i が前記セッション鍵を生成する鍵生成手段と、

を有し、

前記同種写像計算手段は、

N が奇数である場合、前記端末装置 U_i のうち、予め決められた所定の端末装置 U_i が前記第1のねじれ部分群の基底を用いた第1の公開値と、前記第2のねじれ部分群の基底を用いた第2の公開値とを計算する、ことを特徴とする鍵配信システム。

[請求項2]

N (ただし、 $N \geq 2$) 台の端末装置 U_i ($i = 1, \dots, N$) と、該 N 台の端末装置 U_i 間で同種写像暗号によるセッション鍵の交換に用いられる鍵配信サーバとが含まれる鍵配信システムであって、

前記端末装置 U_i が所定の楕円曲線の第1のねじれ部分群の基底を

用いた第1の公開値と、前記楕円曲線の第2のねじれ部分群の基底を用いた第2の公開値とを計算する同種写像計算手段と、

前記鍵配信サーバが、前記端末装置 U_i により計算された第1の公開値と第2の公開値とをそれぞれ端末装置 U_{i-1} （ただし、 $i=1$ である場合、 $U_0=U_N$ ）及び端末装置 U_{i+1} （ただし、 $i=N$ である場合、 $U_{N+1}=U_1$ ）に配信する配信手段と、

前記配信手段により配信された第1の公開値及び第2の公開値を用いて、前記端末装置 U_i が前記セッション鍵を生成する鍵生成手段と、

を有することを特徴とする鍵配信システム。

[請求項3]

前記同種写像計算手段は、

前記第1のねじれ部分群の基底を $\{P_A, Q_A\}$ 、前記第2のねじれ部分群の基底を $\{P_B, Q_B\}$ 、前記第1のねじれ部分群に関する第1のねじれ疑似ランダム関数値を m_i 、前記第1のねじれ部分群に関する第2のねじれ疑似ランダム関数値を n_i 、 $[m_i]P_A + [n_i]Q_A$ で生成される前記楕円曲線の部分群を核に持つ同種写像 ϕ_i とした場合に、前記第1の公開値として、 $\phi_i(P_B)$ 及び $\phi_i(Q_B)$ を計算し、

前記第2のねじれ部分群に関する第3のねじれ疑似ランダム関数値を m'_i 、前記第2のねじれ部分群に関する第4のねじれ疑似ランダム関数値を n'_i 、 $[m'_i]P_B + [n'_i]Q_B$ で生成される前記楕円曲線の部分群を核に持つ同種写像 ϕ'_i とした場合に、前記第2の公開値として、 $\phi'_i(P_A)$ 及び $\phi'_i(Q_A)$ を計算する、

ことを特徴とする請求項1又は2に記載の鍵配信システム。

[請求項4]

前記鍵生成手段は、

前記配信手段により配信された第1の公開値 $\phi_{i-1}(P_B)$ 及び $\phi_{i-1}(Q_B)$ 並びに $\phi_{i+1}(P_B)$ 及び $\phi_{i+1}(Q_B)$ が配信された場合、 $[m_i]\phi_{i-1}(P_B) + [n_i]\phi_{i-1}(Q_B)$ で生成される楕円曲

線の部分群を核に持つ同種写像に付随する楕円曲線の第1のj不変量と、 $[m_i] \phi_{i+1}(P_B) + [n_i] \phi_{i+1}(Q_B)$ で生成される楕円曲線の部分群を核に持つ同種写像に付随する楕円曲線の第2のj不変量とを計算し、計算された第1のj不変量及び第2のj不変量を用いて前記セッション鍵を生成し、

前記配信手段により配信された第2の公開値 $\phi_{i-1}(P_A)$ 及び $\phi_{i-1}(Q_A)$ 並びに $\phi_{i+1}(P_A)$ 及び $\phi_{i+1}(Q_A)$ が配信された場合、 $[m'_i] \phi'_{i-1}(P_A) + [n'_i] \phi'_{i-1}(Q_A)$ で生成される楕円曲線の部分群を核に持つ同種写像に付随する楕円曲線の第3のj不変量と、 $[m'_i] \phi'_{i+1}(P_A) + [n'_i] \phi'_{i+1}(Q_A)$ で生成される楕円曲線の部分群を核に持つ同種写像に付随する楕円曲線の第4のj不変量とを計算し、計算された第3のj不変量及び第4のj不変量を用いて前記セッション鍵を生成する、

ことを特徴とする請求項3に記載の鍵配信システム。

[請求項5] 同種写像暗号によるセッション鍵の交換に用いられる鍵配信サーバと接続される端末装置であって、

所定の楕円曲線の第1のねじれ部分群の基底を用いた第1の公開値又は／及び前記楕円曲線の第2のねじれ部分群の基底を用いた第2の公開値を計算する同種写像計算手段と、

前記セッション鍵を共有する1以上の他の端末装置のうち、所定の2台の端末装置でそれぞれ計算された第1の公開値又は／及び第2の公開値を前記鍵配信サーバから受信する受信手段と、

前記受信手段が受信した第1の公開値又は／及び第2の公開値を用いて、前記セッション鍵を生成する鍵生成手段と、

を有することを特徴とする端末装置。

[請求項6] N (ただし、 $N \geq 2$) 台の端末装置 U_i ($i = 1, \dots, N$) と、該 N 台の端末装置 U_i 間で同種写像暗号によるセッション鍵の交換に用いられる鍵配信サーバとが含まれる鍵配信システムによる鍵配信

方法であって、

N が偶数である場合、前記端末装置 U_i のうち、奇数番目の端末装置 U_i ($i = 1, \dots, N-1$) が所定の楕円曲線の第1のねじれ部分群の基底を用いた第1の公開値を計算し、偶数番目の端末装置 U_i ($i = 2, \dots, N$) が前記楕円曲線の第2のねじれ部分群の基底を用いた第2の公開値を計算する同種写像計算手順と、

前記鍵配信サーバが、奇数番目の端末装置 U_i により計算された第1の公開値を端末装置 U_{i-1} (ただし、 $i = 1$ である場合、 $U_0 = U_N$) 及び端末装置 U_{i+1} (ただし、 $i = N$ である場合、 $U_{N+1} = U_1$) に配信し、偶数番目の端末装置 U_i により計算された第2の公開値を端末装置 U_{i-1} 及び端末装置 U_{i+1} に配信する配信手順と、

前記配信手順により配信された第2の公開値を用いて奇数番目の端末装置 U_i が前記セッション鍵を生成し、前記配信手順により配信された第1の公開値を用いて偶数番目の端末装置 U_i が前記セッション鍵を生成する鍵生成手順と、

を有し、

前記同種写像計算手順は、

N が奇数である場合、前記端末装置 U_i のうち、予め決められた所定の端末装置 U_1 が前記第1のねじれ部分群の基底を用いた第1の公開値と、前記第2のねじれ部分群の基底を用いた第2の公開値とを計算する、ことを特徴とする鍵配信方法。

[請求項7]

N (ただし、 $N \geq 2$) 台の端末装置 U_i ($i = 1, \dots, N$) と、該 N 台の端末装置 U_i 間で同種写像暗号によるセッション鍵の交換に用いられる鍵配信サーバとが含まれる鍵配信システムによる鍵配信方法であって、

前記端末装置 U_i が所定の楕円曲線の第1のねじれ部分群の基底を用いた第1の公開値と、前記楕円曲線の第2のねじれ部分群の基底を用いた第2の公開値とを計算する同種写像計算手順と、

前記鍵配信サーバが、前記端末装置 U_i により計算された第1の公開値と第2の公開値とをそれぞれ端末装置 U_{i-1} （ただし、 $i=1$ である場合、 $U_0=U_N$ ）及び端末装置 U_{i+1} （ただし、 $i=N$ である場合、 $U_{N+1}=U_1$ ）に配信する配信手順と、

前記配信手順により配信された第1の公開値及び第2の公開値を用いて、前記端末装置 U_i が前記セッション鍵を生成する鍵生成手順と

、

を有することを特徴とする鍵配信方法。

[請求項8]

同種写像暗号によるセッション鍵の交換に用いられる鍵配信サーバと接続される端末装置を、

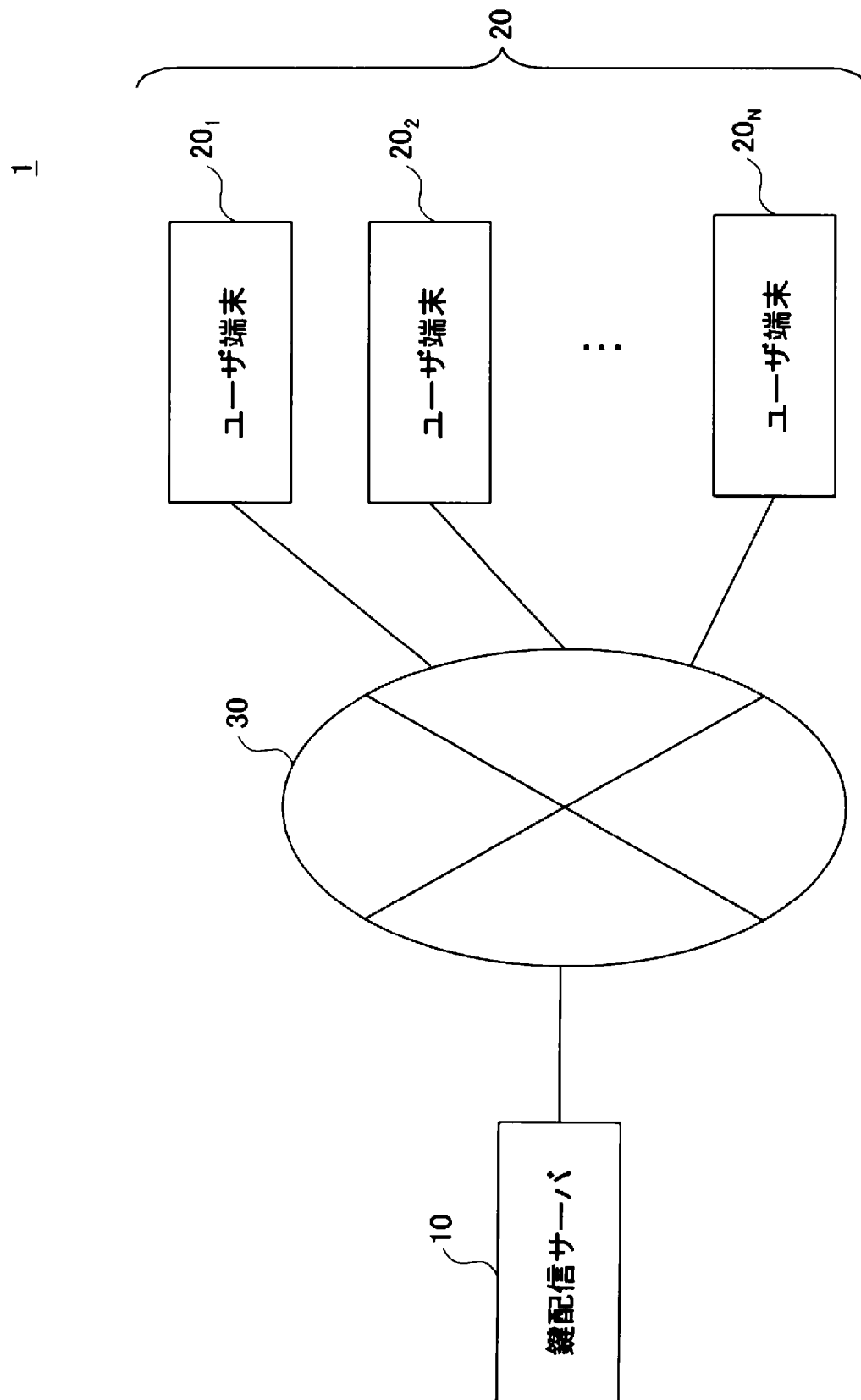
所定の楕円曲線の第1のねじれ部分群の基底を用いた第1の公開値又は／及び前記楕円曲線の第2のねじれ部分群の基底を用いた第2の公開値を計算する同種写像計算手段、

前記セッション鍵を共有する1以上の他の端末装置のうち、所定の2台の端末装置でそれぞれ計算された第1の公開値又は／及び第2の公開値を前記鍵配信サーバから受信する受信手段、

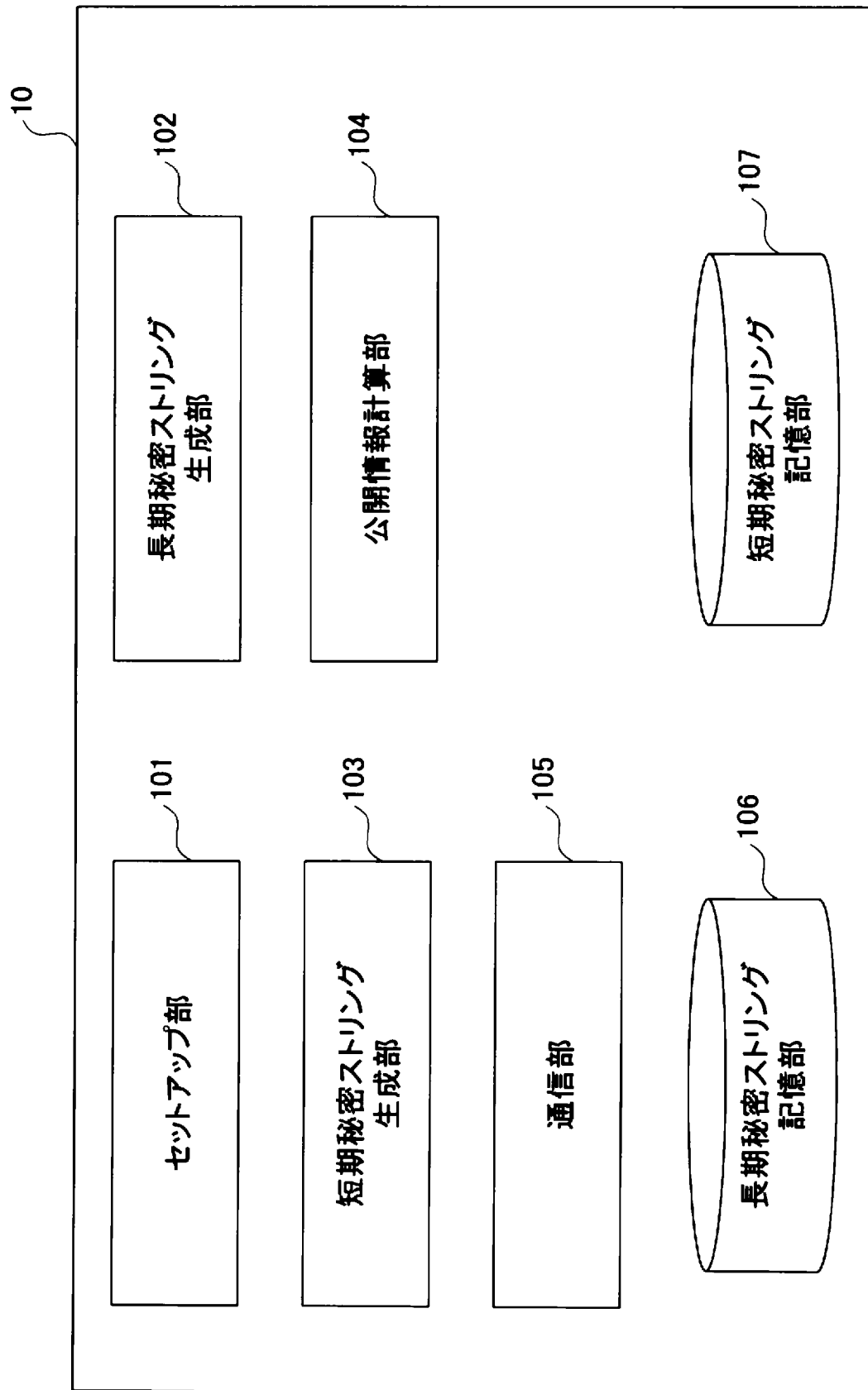
前記受信手段が受信した第1の公開値又は／及び第2の公開値を用いて、前記セッション鍵を生成する鍵生成手段、

として機能させるためのプログラム。

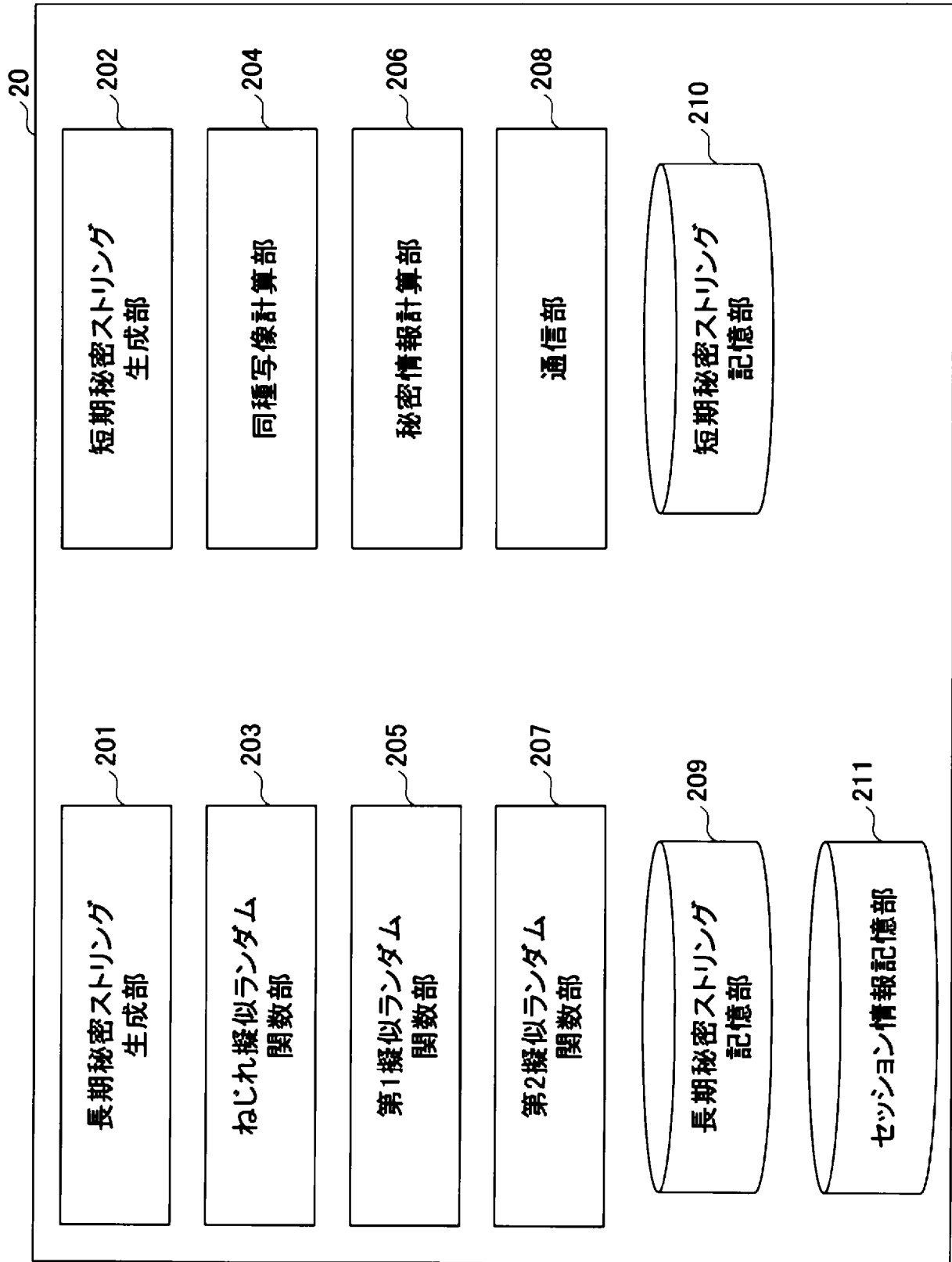
[図1]



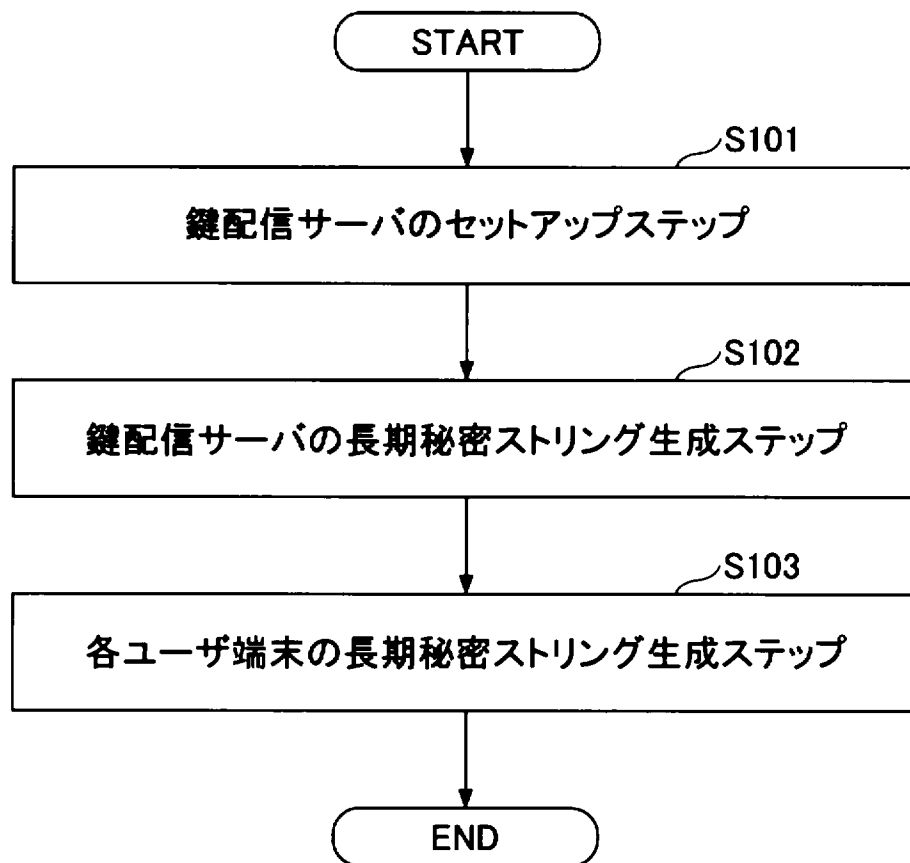
[図2]



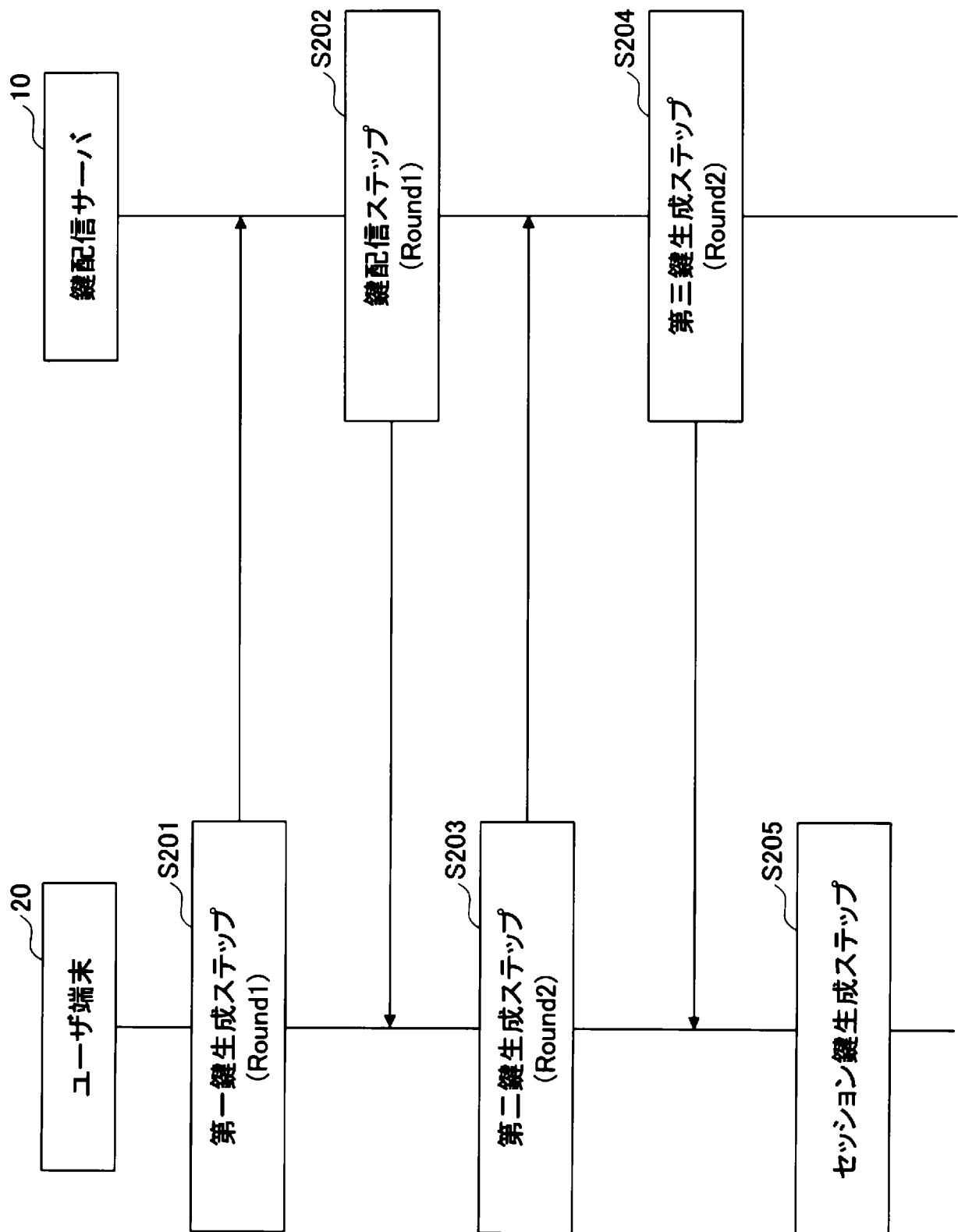
[図3]



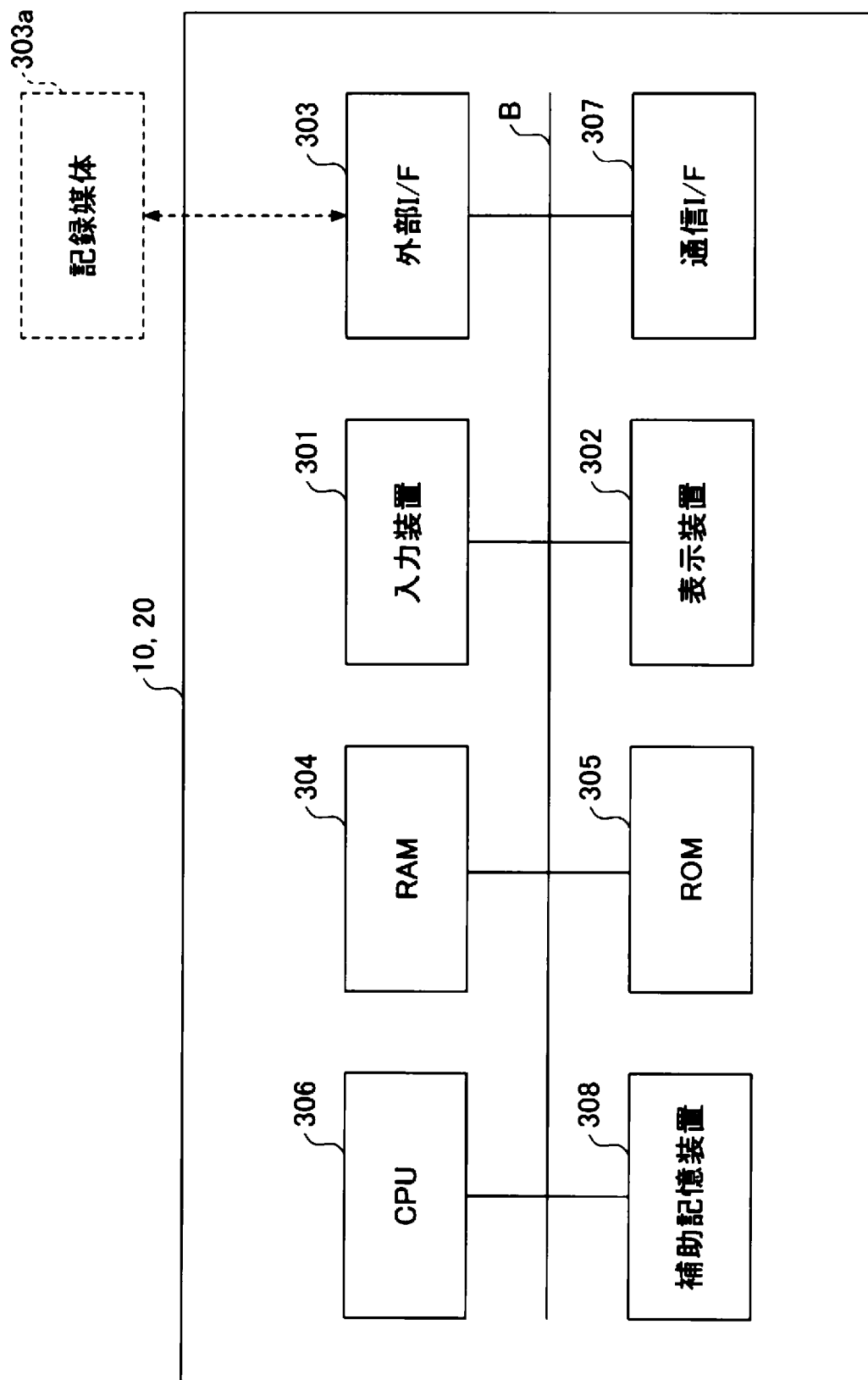
[図4]



[図5]



[図6]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/013412

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. H04L9/08 (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)

Int.Cl. 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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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	古川 悟, 國廣 昇, 高島克幸, 同種写像を用いたグループ鍵共有, SCIS 2016 [USB] SCIS 2016 2016 Symposium on Cryptography and Information Security, 19 January 2016, pp. 1-8, non-official translation (FURUKAWA, Satoru, KUNIHIRO, Noboru, TAKASHIMA, Katsuyuki, "Group Key Sharing Using Isogenies")	1-8

☐ 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

"I" 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
14 June 2019 (14.06.2019)

Date of mailing of the international search report
25 June 2019 (25.06.2019)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. H04L9/08 (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 (IPC))

Int.Cl. 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	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019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	古川 悟, 國廣 昇, 高島 克幸, 同種写像を用いたグループ鍵共有, SCIS2016 [USB] SCIS2016 2016 Symposium on Cryptography and Information Security, 2016.01.19, pp. 1-8	1-8

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	「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
「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	「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
「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)	「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
「O」 口頭による開示、使用、展示等に言及する文献	「&」 同一パテントファミリー文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願	

国際調査を完了した日

14.06.2019

国際調査報告の発送日

25.06.2019

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

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)

打出 義尚

5 S

4440

電話番号 03-3581-1101 内線 3546