(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
2008 年12 月4 日 (04.12.2008)

PCT

(10) 国際公開番号
WO 2008/146547 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2008/057507

(22) 国際出願日: 2008 年4 月17 日 (17.04.2008)

(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2007-138940 2007 年5 月25 日 (25.05.2007) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７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): 古川 潤 (FURUKAWA, Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). アルムクネヒト フレデリク (ARMKNECHT, Frederik) [DE/DE]; 69115 ハイデルベルク クアフェアステンアンラーゲ ３６ エヌイーシー ヨーロッパ リミテッド内 Heidelberg (DE). ジラオ ジョアオ (GIRAO, Joao) [PT/DE]; 69115 ハイデルベルク クアフェアステンアンラーゲ ３６ エヌイーシー ヨーロッパ リミテッド内 Heidelberg (DE).

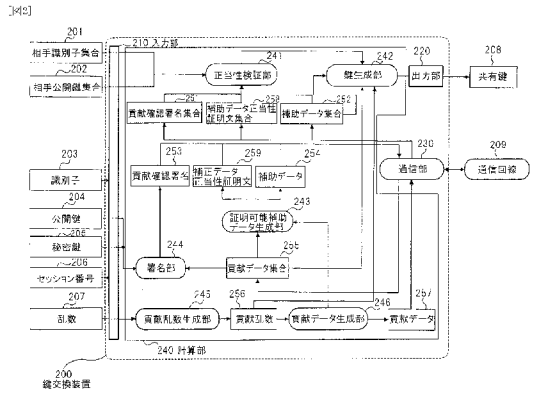
(74) 代理人: 宮崎 昭夫, 外(MIYAZAKI, Teruo et al.); 〒1070052 東京都港区赤坂１丁目９番２０号 第１６興和ビル８階 Tokyo (JP).

(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, JP, KE, KG, KM,

[続葉有]

(54) Title: KEY EXCHANGE DEVICE AND KEY EXCHANGE METHOD

(54) 発明の名称: 鍵交換装置及び鍵交換方法



201 PARTNER IDENTIFIER SET
202 PARTNER PUBLIC KEY SET
203 IDENTIFIER
204 PUBLIC KEY
205 SECRET KEY
206 SESSION NUMBER
207 RANDOM NUMBER
200 KEY EXCHANGE DEVICE
210 INPUT UNIT
241 VALIDITY VERIFYING UNIT
242 KEY GENERATION UNIT
220 OUTPUT UNIT
208 SHARED KEY
251 CONTRIBUTION CHECK SIGNATURE SET
258 AUXILIARY DATA VALIDITY CERTIFICATE SET
252 AUXILIARY DATA SET
253 CONTRIBUTION CHECK SIGNATURE
259 AUXILIARY DATA VALIDITY CERTIFICATE
254 AUXILIARY DATA
230 COMMUNICATION UNIT
209 COMMUNICATION LINE
243 UNIT FOR GENERATING AUXILIARY DATA WHICH CAN BE CONFIRMED
244 SIGNATURE UNIT
255 CONTRIBUTING DATA SET
245 CONTRIBUTING RANDOM NUMBER GENERATION UNIT
256 CONTRIBUTING RANDOM NUMBER
246 CONTRIBUTING DATA GENERATION UNIT
257 CONTRIBUTING DATA
240 CALCULATION UNIT

(57) Abstract: Provided is a key exchange method which communicates with a plurality of partner devices identified by identifiers belonging to a partner identifier set. A public key, a secret key, an identifier, a partner public key set, a partner identifier set, a session number, and a random number are inputted to the partner devices. The method includes steps of: generating a contributing random number by using a random number; generating contributing data by the contributing random number; transmitting the contributing data to the plurality of partner devices; generating a contribution check signature as a signature for the contributing data set formed by all the contributing data received from the partner devices by using the secret key and the public key; generating auxiliary data and an auxiliary data validity certificate by the contributing data set and the contributing random number; sending the auxiliary data, the auxiliary data validity certificate, and the contribution check signature to the partner devices; verifying validity of the auxiliary data by using the partner identifier set and the partner public key set as well as the contribution check signature set, the auxiliary data set, and the auxiliary data validity certificate set which are formed by data received from the partner devices; and generating a shared key by the contributing data set and the auxiliary data which have been received from the partner devices.

(57) 要約: 公開鍵、秘密鍵、識別子、相手公開鍵集合、相手識別子集合、セッション番号及び乱数が入力され、相手識別子集合に属する識別子で識別される複数の相手装置と通信を行い、乱数を用いて貢献乱数を生成し、貢献乱数により貢献データを生

[続葉有]

WO 2008/146547 A1

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, 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, 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, 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

成し、貢献データを複数の相手装置に送付し、秘密鍵と公開鍵を用いて、複数の相手装置から受け取った貢献データの全てよりなる貢献データ集合に対する署名である貢献確認署名を生成し、貢献データ集合と貢献乱数とにより、補助データ及び補助データ正当性証明文を生成し、補助データ、補助データ正当性証明文及び貢献確認署名を、複数の相手装置に送付し、相手識別子集合及び相手公開鍵集合と、複数の相手装置から受け取ったデータからなる貢献確認署名集合、補助データ集合及び補助データ正当性証明文集合とより、補助データの正当性を検証し、複数の相手装置から受け取った貢献データ集合と補助データとにより共有鍵を生成する。

明 細 書

鍵交換装置及び鍵交換方法

技術分野

[0001] 本発明は、互いに通信を行うことにより同一の鍵を交換可能な鍵交換装置及び鍵交換方法に関する。

背景技術

[0002] グループ鍵交換装置として、"Jonathan Katz, Ji Sun Shin: Modeling insider attacks on group key-exchange protocols. ACM Conference on Computer and Communications Security 2005: 180-189"に開示された方式がある。

[0003] 以下に、上記文献に開示された方式について説明する。

[0004] まず、記法を示す。pを素数、G_Tを位数、qの巡回群とする。鍵を交換する装置の数をnとし、それぞれの装置にiで番号を振る。装置iを表す識別子をU[i]とする。GはG_Tの生成子とする。v, wを無作為に選ばれた整数とする。F, F'を擬似乱数生成装置とする。

[0005] 図1は、鍵交換装置の一例を示す図である。

[0006] 本例におけるグループ鍵交換装置は図1に示すように、検証データ検証部311と、検証データ生成部312と、一時鍵生成部313と、補助データ生成部314と、貢献乱数生成部315と、貢献データ生成部316と、通信部317とから構成されている。

[0007] 上記のように構成された鍵交換装置300(i)においては、j={1, ・・・, n}￥iのそれぞれの装置jに対応する識別子の集合である相手識別子集合301と、公開鍵pk[j]の集合である相手公開鍵集合302が入力される。また、識別子303(U[i])と公開鍵304(pk[i])に対応する秘密鍵305(sk[i])も入力される。さらに、これから生成する鍵に固有のセッション番号306(sid)が入力される。

[0008] 鍵交換装置300(i)は、貢献乱数生成部315において、入力された乱数307を用いて貢献乱数324(r[i]∈Z／qZ)をランダムに生成する。

[0009] そして、貢献データ生成部316において、貢献乱数生成部315にて生成された貢献乱数324(r[i]∈Z／qZ)を用いて貢献データ325($y[i]=g^{r[i]}$)生成し、また、sid,

1, U[i], y[i]に対する署名sig(i, 1)を生成する。そして、その他の(n－1)個の装置に対して、(sid, 1, U[i], y[i], sig(i, 1))を通信部317から送付する。

[0010] 鍵交換装置300(i)は、j＝{1, ・・・, n}￥iに関して、装置jが貢献データy[j]を通信回線309を介して送付してくるのを通信部317にて待つ。

[0011] 全ての貢献データy[j]が揃った貢献データ集合323となれば、鍵交換装置300(i)は各署名を検証する。

[0012] 次に、補助データ生成部314において、貢献データ集合323を用いて補助データ322(x[i]＝(y[i＋1]／y[i－1])$^{r[i]}$)を生成し、(sid, 2, U[i], x[i])に対する署名sig(i, 2)を生成する。

[0013] そして、通信部317において、(sid, 2, U[i], x[i], sig(i, 2))をその他の(n－1)個の装置に送付する。

[0014] 通信部317を介して全てのx[j]が受信され、全てのx[j]が揃った補助データ集合321となれば、鍵交換装置300(i)は各署名を検証する。

[0015] 次に、一時鍵生成部313において、k[i]＝(y[i－1]$^{r[i]}$)^{n}×[i＋1]^{n}×[i＋2]$^{n-1}$・・・×[n]$^{i+1}$×[1]^{i}・・・×[i－1]^{2}×[i]を生成する。

[0016] 次に、検証データ生成部312において、ack[i]＝F(k[i], v)を生成し、また、一時鍵生成部313において、共有鍵308(sk[i]＝F'(k[i], w))を生成する。また、(sid[i], 3, U[i], ack[i])に対する署名sig(i, 3)を生成する。

[0017] そして、通信部317において、(sid, 3, U[i], ack[i], sig(i, 3))をその他の(n－1)個の装置に送付する。

[0018] 通信部317を介して全てのack[j]が受信され、全てのack[j]が揃ったならば、鍵交換装置300(i)は、検証データ検証部311において各署名を検証する。

[0019] そして、検証データ検証部311において、全てのj＝{1, ・・・, n}￥iに関して、ack[j]＝ack[i]を確認した場合、一時鍵生成部313から共有鍵308(sk[i])を出力する。

[0020] 上述した技術においては、共有鍵を交換する際、各装置が他の全ての装置に対してデータを3回配布する必要がある。この全ての装置における全ての装置に対するデータの配布が完了しなければ次のステップに移ることができないため、このデータ

の配布に要する時間は、各データの計算に必要な時間に比べて著しく長くなる。ここで、対多数の通信は、その同期を取る処理等に多くの時間を費やすため、単純な暗号計算と比べて短時間で終了することは難しい。そのため、複数、特に、多数の装置間における鍵交換を迅速に行うためには、このようなデータの配布回数を削減する必要がある。

発明の開示

[0021] 本発明は、複数の装置間にて鍵交換を迅速に行うことができる鍵交換装置を提供することを目的とする。

[0022] 上記目的を達成するために本発明は、

公開鍵、秘密鍵、識別子、相手公開鍵集合、相手識別子集合、セッション番号及び乱数が入力され、前記相手識別子集合に属する識別子で識別される複数の相手装置と通信を行い、共有鍵を生成、出力する鍵交換装置であって、

前記乱数を用いて貢献乱数を生成する貢献乱数生成部と、

前記貢献乱数生成部にて生成された貢献乱数により貢献データを生成する貢献データ生成部と、

前記貢献データを前記複数の相手装置に送付する通信部と、

前記秘密鍵と前記公開鍵を用いて、前記複数の相手装置から前記通信部にて受け取った貢献データの全てよりなる貢献データ集合に対する署名である貢献確認署名を生成する署名部と、

前記貢献データ集合と前記貢献乱数とにより、補助データ及び補助データ正当性証明文を生成する証明可能補助データ生成部とを有し、

前記補助データ、前記補助データ正当性証明文及び前記貢献確認署名は、前記通信部により前記複数の相手装置に送付され、

前記相手識別子集合及び前記相手公開鍵集合と、前記複数の相手装置から前記通信部にて受け取ったデータからなる前記貢献確認署名集合、前記補助データ集合及び前記補助データ正当性証明文集合とより、前記補助データの正当性を検証する正当性検証部と、

前記複数の相手装置から前記通信部にて受け取った前記貢献データ集合と前記

補助データとにより前記共有鍵を生成する鍵生成部とを有する。

[0023] 本発明は、以上説明したように構成されているので、複数の装置間にて秘密の鍵を共有する場合に、互いにデータを配布する回数が従来よりも1回少ない2回で済むこととなり、より迅速な鍵の交換が可能になる。

図面の簡単な説明

[0024] [図1]鍵交換装置の一例を示す図である。

[図2]本発明の鍵交換装置の第1の実施の形態を示す図である。

[図3]本発明の鍵交換装置の第2の実施の形態を示す図である。

発明を実施するための最良の形態

[0025] 以下に、本発明の実施の形態について図面を参照して説明する。

[0026] (実施の形態で使われる記法)

pを素数、GとG_Tを位数pの巡回群、eをG掛けるGからG_Tへの非縮退な双線形写像であるとする。ここで双線形であるとは、すべてのα, $\beta \in Z/qZ$及び$g \in G$に対して、

$$e(g^{\alpha}, g^{\beta}) = e(g, g)^{\alpha\beta}$$

が成り立つことである。また、非縮退であるとは、gがGの生成元であるとき、e(g, g)が、G_Tの生成元となるということである。

[0027] 鍵を交換する装置の数をnとし、それぞれの装置にiで番号を振る。装置iを表す識別子をU[i]とする。g, hはG_Tの生成子とする。

[0028] (第1の実施の形態)

図2は、本発明の鍵交換装置の第1の実施の形態を示す図である。

[0029] 本形態における鍵交換装置は図2に示すように、入力部110と計算部140と出力部120と通信部130とから構成され、計算部140は、正当性検証部141と鍵生成部142と証明可能補助データ生成部143と署名部144と貢献乱数生成部145と貢献データ生成部146とを有している。

[0030] 入力部110は、相手識別子集合101、相手公開鍵集合102、識別子103、公開鍵104、秘密鍵105、セッション番号106及び乱数107が入力される。

[0031] 計算部140は、同じ位数の群G, G_Tで、群Gに属する2つの要素から群G_Tへの双

線形写像が存在する二つの群G, G_Tの計算手段であって、入力部110を介して入力された相手識別子集合101、相手公開鍵集合102、識別子103、公開鍵104、秘密鍵105、セッション番号106及び乱数107、並びに通信部130にて受信されたデータを用いて共有鍵108を生成する。

[0032] 出力部120は、計算部140にて生成された共有鍵108を出力する。

[0033] 貢献乱数生成部145は、入力部110を介して入力された乱数107を用いて、貢献データ157を生成するための乱数である貢献乱数156を生成する。

[0034] 貢献データ生成部146は、貢献乱数生成部145にて生成された貢献乱数156より貢献データ157を生成する。

[0035] 署名部144は、入力部110を介して入力された秘密鍵105と公開鍵104を用いて、全ての相手装置から受け取った全ての貢献データよりなる貢献データ集合155に対する署名となる貢献確認署名153を生成する。

[0036] 証明可能補助データ生成部143は、貢献データ集合155と貢献乱数156とにより、補助データ154を生成する。

[0037] 正当性検証部141は、入力部110を介して入力された相手識別子集合101と相手公開鍵集合102と、通信部130を介して全ての相手装置から受け取ったデータからなる貢献確認署名集合151及び補助データ集合152とから、補助データの正当性を確認する。

[0038] 鍵生成装置142は、通信部130を介して全ての相手装置から受け取った貢献データ集合155及び補助データ集合152から共有鍵108を生成する。

[0039] 通信部130は、通信回線109を介して相手装置とデータ交換するためのものであって、貢献データ生成部146にて生成された貢献データ157と、証明可能補助データ生成部143にて生成された補助データ154と、署名部144にて生成された貢献確認署名153とを通信回線109を介して全ての相手装置に送付する。

[0040] 以下に、上記のように構成された鍵交換装置100の動作について説明する。

[0041] 鍵交換装置100(i)のそれぞれには、j={1, ・・・, n}￥iのそれぞれの装置jに対応する識別子U[j]の集合である相手識別子集合101と、j={1, ・・・, n}￥iのそれぞれの装置jに対応する公開鍵pk[j]の集合である相手公開鍵集合102とが入力部11

0を介して入力される。また、自身の装置に対応する識別子103と、自身の公開鍵104(pk[i])と、この公開鍵104(pk[i])に対応する秘密鍵105(sk[i])も入力部110を介して入力される。さらに、これから生成される共有鍵108に固有のセッション番号106(sid)と乱数107が入力部110を介して入力される。

[0042] 鍵交換装置100(i)は、まず、貢献乱数生成部145において、入力部110を介して入力された乱数107を用いて、貢献データ157を生成するための乱数である貢献乱数156(r[i]∈Z／qZ)をランダムに生成する。

[0043] 次に、貢献データ生成部146において、貢献乱数生成部145にて生成された貢献乱数156から貢献データ157($y[i]=g^{r[i]}$)を生成し、この貢献データ157($y[i]=g^{r[i]}$)を通信部130において、その他の(n－1)個の装置に送付する。

[0044] 鍵交換装置100(i)は、j＝{1, ･･･, n}￥iに関して、装置jが貢献データy[j]を送付してくるのを通信部130にて待つ。

[0045] 通信部130にて全ての装置からの貢献データy[j]が受信され、全ての貢献データy[j]が揃った貢献データ集合155となると、証明可能補助データ生成部143において、貢献データ集合155と貢献乱数156とにより補助データ154($x[i]=(y[i+1]／y[i-1])^{r[i]}$)を生成し、また、署名部144において、入力部110を介して入力された秘密鍵105と公開鍵104を用いて、全ての相手装置から受け取った全ての貢献データよりなる貢献データ集合155(sid, y[1], ･･･, y[n])に対する署名である貢献確認署名153(sig)を生成する。

[0046] そして、通信部130において、(sid, x[i], sig)をその他の(n－1)個の装置に送付する。

[0047] 通信部130にて全ての装置からの補助データx[j]が受信され、全ての補助データx[j]が揃った補助データ集合152となると、正当性検証部141において、入力部110を介して入力された相手識別子集合101と相手公開鍵集合102と、他の装置から送られてきて通信部130にて受信されたデータからなる貢献確認署名集合151及び補助データ集合152とから、貢献確認署名集合151の各署名を検証する。

[0048] 次に、鍵生成部142において、通信部130を介して全ての相手装置から受け取った貢献データ集合155及び補助データ集合152から$sk[i]=(y[i-1]^{r[i]})^n\times[i+1]^n$

$\times[i+2]^{n-1}\cdots\times[n]^{i+1}\times[1]^{i}\cdots\times[i-1]^{2}\times[i]$を生成する。

[0049] そして、正当性検証部141において、$e(k[i], g)=e(y[n], y[1])\prod_{j}^{n-1}e(y[j], y[j+1])$が成り立つことを確認し、成り立てば、鍵生成部142から共有鍵108($sk[i]=e(g, h)$)を出力部120を介して出力する。

[0050] (第2の実施の形態)

本形態は、第1の実施の形態とは異なり、Gに双線形写像が存在しないものとする。

[0051] 図3は、本発明の鍵交換装置の第2の実施の形態を示す図である。

[0052] 本形態における鍵交換装置は図3に示すように、入力部210と計算部240と出力部220と通信部230とから構成され、計算部240は、正当性検証部241と鍵生成部242と証明可能補助データ生成部243と署名部244と貢献乱数生成部245と貢献データ生成部246とを有している。

[0053] 入力部210は、相手識別子集合201、相手公開鍵集合202、識別子203、公開鍵204、秘密鍵205、セッション番号206及び乱数207が入力される。

[0054] 計算部240は、入力部210を介して入力された相手識別子集合201、相手公開鍵集合202、識別子203、公開鍵204、秘密鍵205、セッション番号206及び乱数207、並びに通信部230にて受信されたデータを用いて共有鍵208を生成する。

[0055] 出力部220は、計算部240にて生成された共有鍵208を出力する。

[0056] 貢献乱数生成部245は、入力部210を介して入力された乱数207を用いて、貢献データ257を生成するための乱数である貢献乱数256を生成する。

[0057] 貢献データ生成部246は、貢献乱数生成部245にて生成された貢献乱数256より貢献データ257を生成する。

[0058] 署名部244は、入力部210を介して入力された秘密鍵205と公開鍵204を用いて、全ての相手装置から受け取った全ての貢献データよりなる貢献データ集合255に対する署名となる貢献確認署名253を生成する。

[0059] 証明可能補助データ生成部243は、貢献データ集合255と貢献乱数256とにより、補助データ254及び補助データ正当性証明文259を生成する。

[0060] 正当性検証部241は、入力部210を介して入力された相手識別子集合201と相手公開鍵集合202と、通信部230を介して全ての相手装置から受け取ったデータから

なる貢献確認署名集合251、補助データ集合252及び補助データ正当性証明文集合258とから、補助データの正当性を確認する。

[0061] 鍵生成装置242は、通信部230を介して全ての相手装置から受け取った貢献データ集合255及び補助データ集合252から共有鍵208を生成する。

[0062] 通信部230は、通信回線209を介して相手装置とデータ交換するためのものであって、貢献データ生成部246にて生成された貢献データ257と、証明可能補助データ生成部243にて生成された補助データ254及び補助データ正当性証明文259と、署名部244にて生成された貢献確認署名253とを通信回線209を介して全ての相手装置に送付する。

[0063] 以下に、上記のように構成された鍵交換装置200の動作について説明する。

[0064] 鍵交換装置200(i)のそれぞれには、j={1, ・・・, n}￥iのそれぞれの装置jに対応する識別子U[j]の集合である相手識別子集合201と、j={1, ・・・, n}￥iのそれぞれの装置jに対応する公開鍵pk[j]の集合である相手公開鍵集合202とが入力部210を介して入力される。また、自身の装置に対応する識別子203と、自身の公開鍵204(pk[i])と、この公開鍵204(pk[i])に対応する秘密鍵205(sk[i])も入力部210を介して入力される。さらに、これから生成される共有鍵208に固有のセッション番号206(sid)と乱数207が入力部210を介して入力される。

[0065] 鍵交換装置200(i)は、まず、貢献乱数生成部245において、入力部210を介して入力された乱数207を用いて、貢献データ257を生成するための乱数である貢献乱数256(r[i]∈Z／qZ)をランダムに生成する。

[0066] 次に、貢献データ生成部246において、貢献乱数生成部245にて生成された貢献乱数256から貢献データ257($y[i]=g^{r[i]}$)を生成し、この貢献データ157($y[i]=g^{r[i]}$)を通信部230において、その他の(n－1)個の装置に送付する。

[0067] 鍵交換装置200(i)は、j={1, ・・・, n}￥iに関して、装置jが貢献データy[j]を送付してくるのを通信部230にて待つ。

[0068] 通信部230にて全ての装置からの貢献データy[j]が受信され、全ての貢献データy[j]が揃った貢献データ集合255となると、証明可能補助データ生成部243において、貢献データ集合255と貢献乱数256とにより補助データ254(x[i]＝(y[i＋1]／

$y[i-1])^{r[i]}$)を生成し、また、署名部244において、入力部210を介して入力された秘密鍵205と公開鍵204を用いて、全ての相手装置から受け取った全ての貢献データよりなる貢献データ集合255(sid, y[1], ・・・, y[n])に対する署名である貢献確認署名253(sig)を生成する。証明可能補助データ生成部243においては、x[i]がy[i+1], y[i-1], r[i]より正しく作られたことを、y[i+1], y[i-1], y[i], gのみを示して、非対話零知識で証明する。この証明文を、補助データ正当性証明文259(proof[i])とする。

[0069] そして、通信部230において、(sid, proof[i], sig)をその他の(n-1)個の装置に送付する。

[0070] 通信部230にて全ての装置からの補助データx[j]が受信され、全ての補助データx[j]が揃った補助データ集合252となると、正当性検証部241において、入力部210を介して入力された相手識別子集合201と相手公開鍵集合202と、他の装置から送られてきて通信部230にて受信されたデータからなる貢献確認署名集合251及び補助データ集合252とから、貢献確認署名集合251の各署名と、補助データ正当性証明文集合258の各補助データ正当性証明文(proof[j])を検証する。

[0071] 次に、鍵生成部242において、通信部230を介して全ての相手装置から受け取った貢献データ集合255及び補助データ集合252から$sk[i]=(y[i-1]^{r[i]})^n\times[i+1]^n\times[i+2]^{n-1}\cdots\times[n]^{i+1}\times[1]^i\cdots\times[i-1]^2\times[i]$を生成する。

[0072] そして、鍵生成部242から共有鍵208(sk[i]=e(g, h))を出力部220を介して出力する。

[0073] 上述した2つの実施の形態においては、各装置が署名を生成する対象の文章が、全て同じである。このような場合、署名を、アグリゲート署名を用い、検証に必要な計算量を減らすことができる。

[0074] なお、本発明においては、鍵交換装置内の処理は上述の専用のハードウェアにより実現されるもの以外に、その機能を実現するためのプログラムを鍵交換装置にて読取可能な記録媒体に記録し、この記録媒体に記録されたプログラムを鍵交換装置に読み込ませ、実行するものであっても良い。鍵交換装置にて読取可能な記録媒体とは、フロッピーディスク、光磁気ディスク、DVD、CDなどの移設可能な記録媒体の他

、鍵交換装置に内蔵されたHDD等を指す。この記録媒体に記録されたプログラムは、例えば、制御ブロックにて読み込まれ、制御ブロックの制御によって、上述したものと同様の処理が行われる。

産業上の利用可能性

[0075] 複数の装置による鍵の交換は、ネットワーク上で多人数のユーザが会議を開く場合などに有効である。参加するメンバが確認でき、メンバ外のユーザが会議に参加したり、会議の内容を盗聴できないようにしたりするために、会議メンバで共有する秘密鍵を、本発明による鍵交換装置を用いて事前に決定することができる。

[0076] 以上、実施例を参照して本願発明を説明したが、本願発明は上記実施例に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解し得る様々な変更をすることができる。

[0077] この出願は、2007年5月25日に出願された日本出願特願2007－138940を基礎とする優先権を主張し、その開示の全てをここに取り込む。

請求の範囲

[1] 公開鍵、秘密鍵、識別子、相手公開鍵集合、相手識別子集合、セッション番号及び乱数が入力され、前記相手識別子集合に属する識別子で識別される複数の相手装置と通信を行い、共有鍵を生成、出力する鍵交換装置であって、

前記乱数を用いて貢献乱数を生成する貢献乱数生成部と、

前記貢献乱数生成部にて生成された貢献乱数により貢献データを生成する貢献データ生成部と、

前記貢献データを前記複数の相手装置に送付する通信部と、

前記秘密鍵と前記公開鍵を用いて、前記複数の相手装置から前記通信部にて受け取った貢献データの全てよりなる貢献データ集合に対する署名である貢献確認署名を生成する署名部と、

前記貢献データ集合と前記貢献乱数とにより、補助データ及び補助データ正当性証明文を生成する証明可能補助データ生成部とを有し、

前記補助データ、前記補助データ正当性証明文及び前記貢献確認署名は、前記通信部により前記複数の相手装置に送付され、

前記相手識別子集合及び前記相手公開鍵集合と、前記複数の相手装置から前記通信部にて受け取ったデータからなる前記貢献確認署名集合、前記補助データ集合及び前記補助データ正当性証明文集合とより、前記補助データの正当性を検証する正当性検証部と、

前記複数の相手装置から前記通信部にて受け取った前記貢献データ集合と前記補助データとにより前記共有鍵を生成する鍵生成部とを有する鍵交換装置。

[2] 請求項1に記載の鍵交換装置において、

同じ位数の群G, G_Tで、群Gに属する2つの要素から群G_Tへの双線形写像が存在する2つの群G, G_Tの計算手段を有し、

前記貢献データ及び前記補助データは群Gの元であって、

前記補助データ正当性証明文は空集合であって、

前記正当性検証部は、前記相手識別子集合及び前記相手公開鍵集合と、前記複数の相手装置から前記通信部にて受け取った前記貢献確認署名集合及び前記補

助データ集合とより、前記補助データの正当性を検証することを特徴とする装置。

[3] 請求項1または請求項2に記載の鍵交換装置において、

前記署名を生成するのに用いる署名方式が、アグリゲート署名であることを特徴とする鍵交換装置。

[4] 公開鍵、秘密鍵、識別子、相手公開鍵集合、相手識別子集合、セッション番号及び乱数が与えられ、前記相手識別子集合に属する識別子で識別される複数の相手装置と通信を行い、共有鍵を生成、出力する鍵交換方法であって、

前記乱数を用いて貢献乱数を生成する処理と、

前記生成された貢献乱数により貢献データを生成する処理と、

前記貢献データを前記複数の相手装置に送付する処理と、

前記秘密鍵と前記公開鍵を用いて、前記複数の相手装置から受け取った貢献データの全てよりなる貢献データ集合に対する署名である貢献確認署名を生成する処理と、

前記貢献データ集合と前記貢献乱数とにより、補助データ及び補助データ正当性証明文を生成する処理と、

前記補助データ、前記補助データ正当性証明文及び前記貢献確認署名を、前記複数の相手装置に送付する処理と、

前記相手識別子集合及び前記相手公開鍵集合と、前記複数の相手装置から受け取ったデータからなる前記貢献確認署名集合、前記補助データ集合及び前記補助データ正当性証明文集合とより、前記補助データの正当性を検証する処理と、

前記複数の相手装置から受け取った前記貢献データ集合と前記補助データとにより前記共有鍵を生成する処理とを有する鍵交換方法。

[5] 公開鍵、秘密鍵、識別子、相手公開鍵集合、相手識別子集合、セッション番号及び乱数が入力され、前記相手識別子集合に属する識別子で識別される複数の相手装置と通信を行い、共有鍵を生成、出力する鍵交換装置に、

前記乱数を用いて貢献乱数を生成する手順と、

前記生成された貢献乱数により貢献データを生成する手順と、

前記貢献データを前記複数の相手装置に送付する手順と、

前記秘密鍵と前記公開鍵を用いて、前記複数の相手装置から受け取った貢献データの全てよりなる貢献データ集合に対する署名である貢献確認署名を生成する手順と、

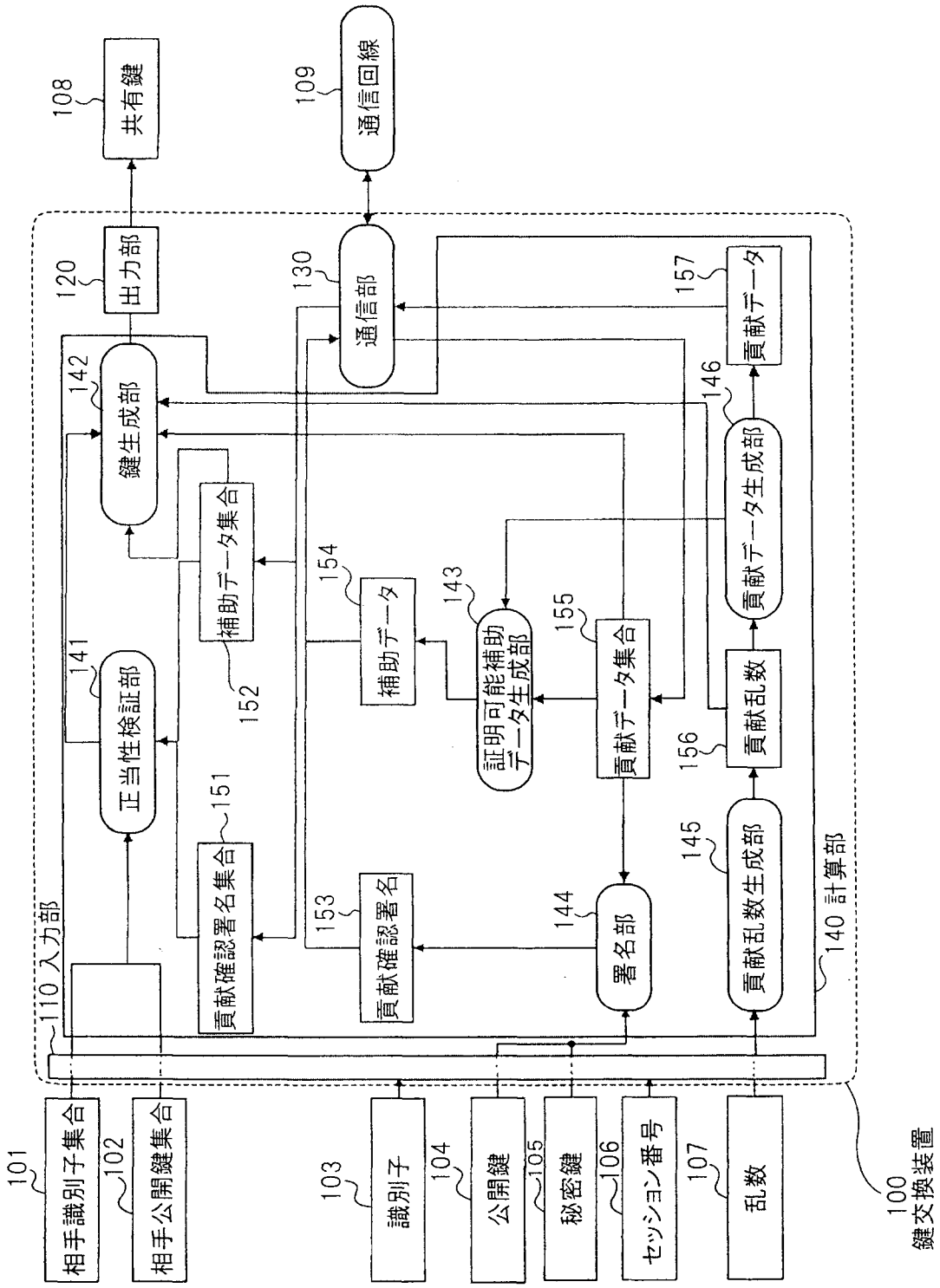
前記貢献データ集合と前記貢献乱数とにより、補助データ及び補助データ正当性証明文を生成する手順と、

前記補助データ、前記補助データ正当性証明文及び前記貢献確認署名を、前記複数の相手装置に送付する手順と、

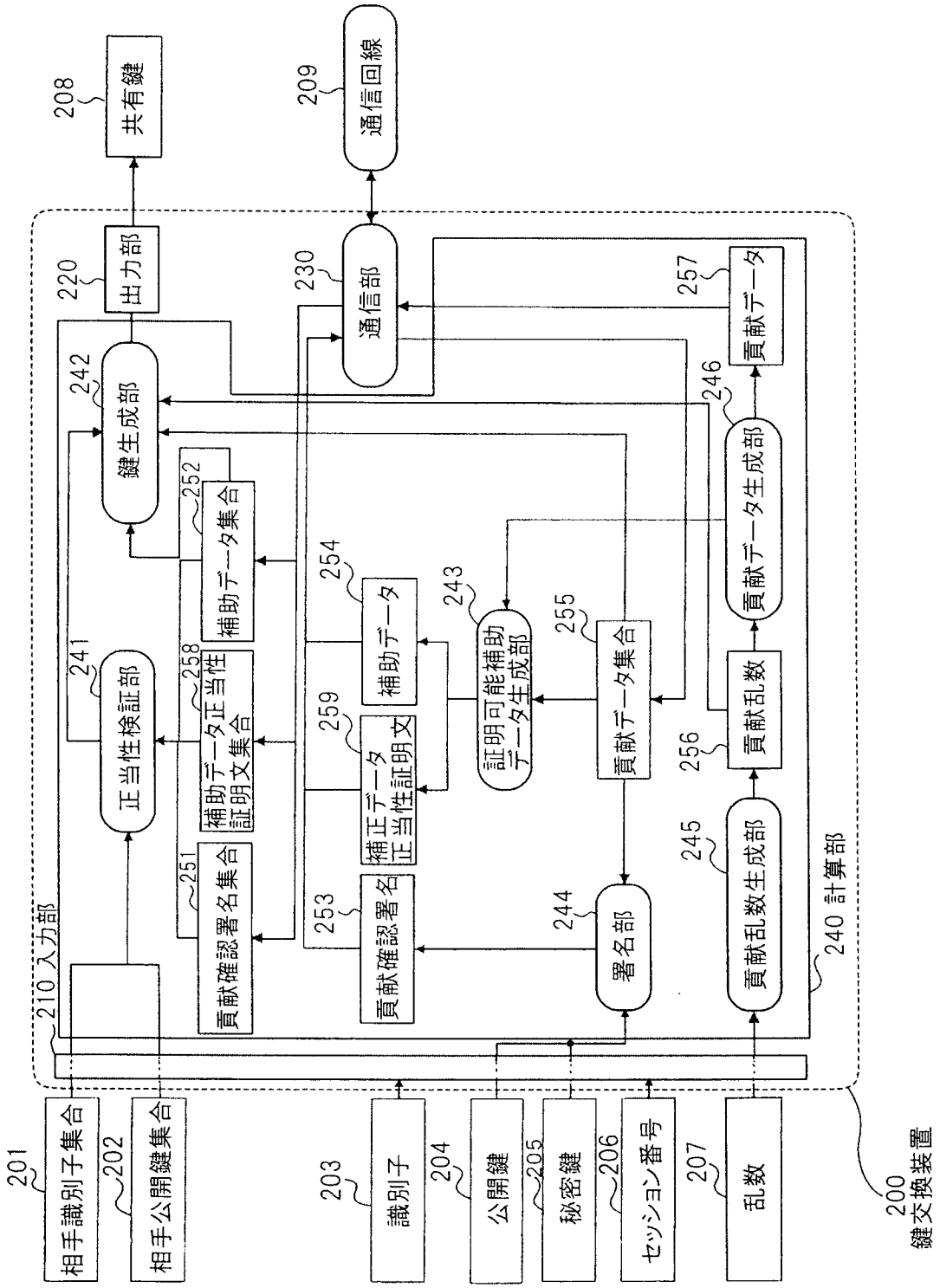
前記相手識別子集合及び前記相手公開鍵集合と、前記複数の相手装置から受け取ったデータからなる前記貢献確認署名集合、前記補助データ集合及び前記補助データ正当性証明文集合とより、前記補助データの正当性を検証する手順と、

前記複数の相手装置から受け取った前記貢献データ集合と前記補助データとにより前記共有鍵を生成する手順とを実行させるためのプログラム。

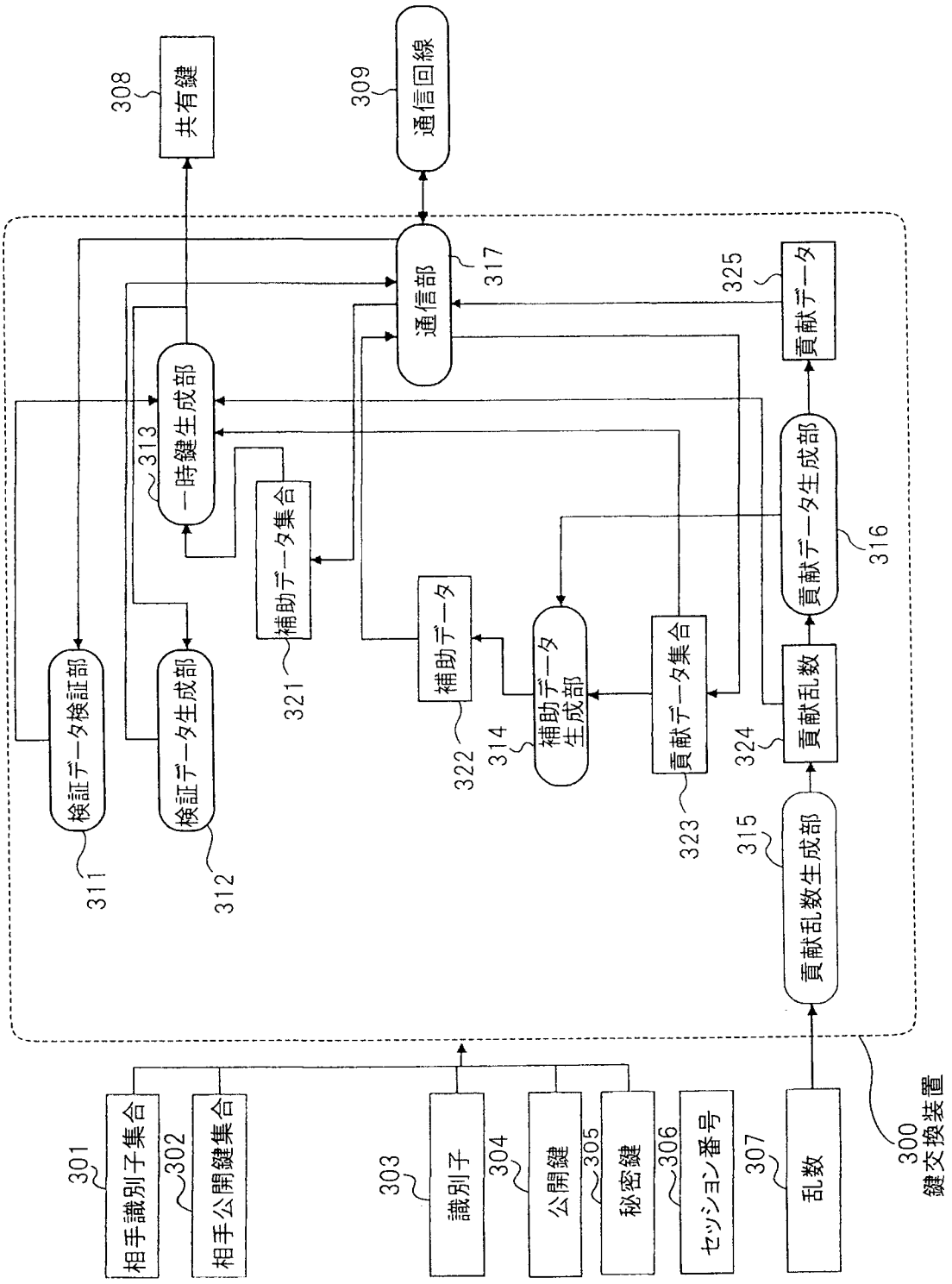
[図1]


100 鍵交換装置
101 相手識別子集合
102 相手公開鍵集合
103 識別子
104 公開鍵
105 秘密鍵
106 セッション番号
107 乱数
108 共有鍵
109 通信回線
110 入力部
120 出力部
130 通信部
140 計算部
141 正当性検証部
142 鍵生成部
143 証明可能補助データ生成部
144 署名部
145 貢献乱数生成部
146 貢献データ生成部
151 貢献確認署名集合
152 補助データ集合
153 貢献確認署名
154 補助データ
155 貢献データ集合
156 貢献乱数
157 貢献データ

[図2]


200 鍵交換装置
201 相手識別子集合
202 相手公開鍵集合
203 識別子
204 公開鍵
205 秘密鍵
206 セッション番号
207 乱数
208 共有鍵
209 通信回線
210 入力部
220 出力部
230 通信部
240 計算部
241 正当性検証部
242 鍵生成部
243 証明可能補助データ生成部
244 署名部
245 貢献乱数生成部
246 貢献データ生成部
251 貢献確認署名集合
252 補助データ集合
253 貢献確認署名
254 補助データ
255 貢献データ集合
256 貢献乱数
257 貢献データ
258 補助データ正当性証明文集合
259 補正データ正当性証明文

[図3]


308
共有鍵
309
通信回線
317
通信部
325
貢献データ
313
一時鍵生成部
316
貢献データ生成部
321
補助データ集合
322
補助データ
314
補助データ生成部
323
貢献データ集合
324
貢献乱数
315
貢献乱数生成部
311
検証データ検証部
312
検証データ生成部
301
相手識別子集合
302
相手公開鍵集合
303
識別子
304
公開鍵
305
秘密鍵
306
セッション番号
307
乱数
300
鍵交換装置

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/057507

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 1996-2008
Kokai Jitsuyo Shinan Koho 1971-2008 Toroku Jitsuyo Shinan Koho 1994-2008

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.
Y	Mike Burmester et.al. "A Secure and Efficient Conference key Distribution System" Advances in Cryptology-EuroCrypt '94 Lecture Notes inComputer Science Springer-Verlag, Vol.1440, 1999, p.275-p.286	1,3-5
Y	JP 2004-280401 A (Toshiba Corp.), 07 October, 2004 (07.10.04), Par. Nos. [0053] to [0057] (Family: none)	1,3-5
Y	Tatsuaki OKAMOTO et al., "Ango Zero Chishiki Shomei Suron", Kyoritsu Shuppan Co., Ltd., 01 June, 1995 (01.06.95), pages 45 to 46	1,3-5

☐ 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
19 May, 2008 (19.05.08)	27 May, 2008 (27.05.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/057507

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.:2
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
Claim 2 has a phrase "to verify validity of the auxiliary data". However, the form of Expression of sk[i] used for verification is not clear in the paragraphs [0048], [0049] of the Description.
(Continued to extra sheet)

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

the

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.II-2 of continuation of first sheet(2)

It is unknown how to verify the validity of the auxiliary data by using the sk[i]. Accordingly, claim 2 is not disclosed sufficiently within the meaning of PCT Article 5 or not supported by disclosure in the Descritpion within the meaning of PCT Article 6.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０５７５０７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

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（ＩＰＣ））

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	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００８年
日本国実用新案登録公報	１９９６－２００８年
日本国登録実用新案公報	１９９４－２００８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	関連する請求の範囲の番号
Y	Mike Burmester et.al. “ A Secure and Efficient Conference key Distribution System” Advances in Cryptology-EuroCrypt ’94 Lecture Notes inComputer Science Springer-Verlag, Vol.1440, 1999, p.275-p.286	1,3-5
Y	JP 2004-280401 A（株式会社東芝）2004.10.07, 【0053】～【0057】段落（ファミリーなし）	1,3-5

☑　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 １９．０５．２００８	国際調査報告の発送日 ２７．０５．２００８
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 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）　５Ｓ　３８５７ 青木　重徳 電話番号　０３－３５８１－１１０１　内線　３５４６

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	関連する請求の範囲の番号
Y	岡本龍明他，暗号・ゼロ知識証明・数論，共立出版株式会社，1995.06.01，p.45-p.46	1,3-5

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０５７５０７

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

１．☐ 請求の範囲＿＿＿＿＿＿＿＿は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

２．☑ 請求の範囲 2 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
請求の範囲２には「補助データの正当性を検証する」とあるが、明細書の【0048】、【0049】段落の記載では、検証に用いるsk[i]の式の形が不明であり、前記sk[i]を用いて何故補助データの正当性を検証できるのか不明であるから、PCT第5条の意味での開示を欠き、またPCT第6条の意味での明細書の開示による裏付けを欠いている。

３．☐ 請求の範囲＿＿＿＿＿＿＿＿は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

１．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

２．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

３．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

４．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。

☐ 追加調査手数料の納付はあったが、異議申立てはなかった。