

(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
2016 年 12 月 15 日(15.12.2016)



(10) 国際公開番号

WO 2016/199507 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01) H04L 9/32 (2006.01)
- (21) 国際出願番号: PCT/JP2016/062601
- (22) 国際出願日: 2016 年 4 月 21 日(21.04.2016)
- (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 2015-116322 2015 年 6 月 9 日(09.06.2015) 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: 吉田 麗生(YOSHIDA, Reo); 〒1808585 東京都武蔵野市緑町三丁目 9 番 1 1 号 N T T 知的財産センタ内 Tokyo (JP). 富士 仁(FUJI, Hitoshi); 〒1808585 東京都武蔵野市緑町三丁目 9 番 1 1 号 N T T 知的財産センタ内 Tokyo (JP).
- (74) 代理人: 中尾 直樹, 外(NAKAO, Naoki et al.); 〒1600022 東京都新宿区新宿三丁目 1 番 2 2 号 新宿 N S O ビル 6 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR,

[続葉有]

(54) Title: KEY EXCHANGE METHOD, KEY EXCHANGE SYSTEM, KEY DISTRIBUTION DEVICE, COMMUNICATION DEVICE, AND PROGRAM

(54) 発明の名称: 鍵交換方法、鍵交換システム、鍵配送装置、通信装置、およびプログラム

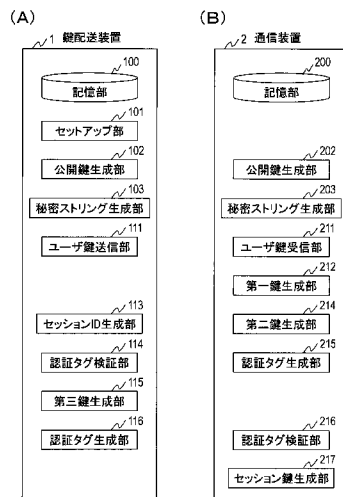


図2

- 1 Key distribution device
2 Communication device
100, 200 Storage unit
101 Setup unit
102, 202 Public key generation unit
103, 203 Secret string generation unit
111 User key transmission unit
113 Session ID generation unit
114, 216 Authentication tag verification unit
115 Third key generation unit
116, 215 Authentication tag generation unit
211 User key reception unit
212 First key generation unit
214 Second key generation unit
217 Session key generation unit

(57) Abstract: The present invention reduces the amount of computation required for key exchange when multiple users are sharing a shared key, while allowing dynamic membership changes. A first key generation unit 212 uses a twist pseudorandom function to calculate R_i, c_i . A session ID generation unit 113 generates sid with a target collision resistant hash function and transmits (sid, R_a, R_b) to a communication device U_i . A second key generation unit 214 of a representative communication unit U_1 uses a pseudorandom function to calculate T_1 . A second key generation unit 214 of a general communication unit U_j uses a pseudorandom function to calculate T_j . A third key generation unit 115 uses a twist pseudorandom function to calculate k' , and calculates T'_j for each j . A session key generation unit 217 of the general communication unit U_j calculates K_j^1, k_1 . The session key generation unit 217 generates a shared key K_2 with a pseudorandom function.

(57) 要約: 動的なメンバ変更を許しながら複数のユーザが共通鍵を共有し、鍵交換に必要な計算量を低減する。第一鍵生成部 212 がねじれ疑似ランダム関数を用いて R_i, c_i を計算する。セッション ID 生成部 113 がターゲット衝突困難ハッシュ関数により sid を生成し、 (sid, R_a, R_b) を通信装置 U_i へ送信する。代表通信装置 U_1 の第二鍵生成部 214 が疑似ランダム関数を用いて T_1 を計算する。一般通信装置 U_j の第二鍵生成部 214 が疑似ランダム関数を用いて T_j を計算する。第三鍵生成部 115 がねじれ疑似ランダム関数を用いて k' を計算し、各 j について T'_j を計算する。一般通信装置 U_j のセッション鍵生成部 217 が K_j^1, k_1 を計算する。セッション鍵生成部 217 が疑似ランダム関数により共通鍵 K_2 を生成する。



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.

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).

- (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

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

鍵交換方法、鍵交換システム、鍵配送装置、通信装置、およびプログラム
技術分野

[0001] この発明は情報セキュリティ技術の応用に関し、特に、グループを形成する複数のユーザが共通鍵を共有する鍵交換技術に関する。

背景技術

[0002] 従来からグループを形成する複数のユーザが共通鍵を共有する鍵交換技術が提案されている（例えば、非特許文献 1、2 参照）。非特許文献 1 には、そのような鍵交換技術を実現する情報システムのアーキテクチャが記載されている。非特許文献 2 には、そのような鍵交換技術のアルゴリズムが記載されている。

先行技術文献

非特許文献

[0003] 非特許文献1：Suvo Mittra, “Iolus: a framework for scalable secure multicasting”, SIGCOMM '97, pp. 277-288

非特許文献2：“Scalable Multicast Key Distribution”、[online]、[平成27年6月5日検索]、インターネット<URL:<https://tools.ietf.org/html/rfc1949>>

発明の概要

発明が解決しようとする課題

[0004] 非特許文献 1、2 に記載の従来技術では、予め共通鍵を共有するユーザを登録しておく必要があるため、動的なメンバ変更を許しながら複数のユーザが共通鍵を共有することはできない。また、ユーザ数を n として、全体として鍵交換に必要な計算量は $O(\log n)$ となるため、ユーザ数の増大に従って鍵交換の計算量が増えるという問題がある。

[0005] この発明の目的は、このような点に鑑みて、動的なメンバ変更を許しながら

ら複数のユーザが共通鍵を共有することができ、鍵交換に必要な計算量を低減することができる鍵交換技術を提供することである。

課題を解決するための手段

[0006] 上記の課題を解決するために、この発明の鍵交換方法は、 n を2以上の整数とし、 i を1から n までの各整数とし、 j を2から n までの各整数とし、 S を鍵配送装置とし、 U_i を n 台の通信装置とし、 U_i を n 台の通信装置 U_i から選択された1台の代表通信装置とし、 U_j を n 台の通信装置 U_i から代表通信装置 U_i を除いた $n-1$ 台の一般通信装置とし、 $||$ を連結演算子とし、 α 、 β を次式で定義される整数とし、

[0007] [数1]

$$\alpha = \begin{cases} i-1 & \text{if } i-1 \geq 1 \\ i-1+n & \text{if } i-1 < 1 \end{cases}$$

$$\beta = \begin{cases} i+1 & \text{if } i+1 \leq n \\ i+1-n & \text{if } i+1 > n \end{cases}$$

[0008] 鍵配送装置 S の記憶部に、鍵配送装置 S の公開鍵暗号の秘密鍵 sk_s および秘密ストリング st_s 、 st'_s が記憶されており、通信装置 U_i の記憶部に、通信装置 U_i の公開鍵暗号の秘密鍵 sk_i および秘密ストリング st_i 、 st'_i が記憶されており、通信装置 U_i が、ねじれ疑似ランダム関数により秘密ストリング st_i 、 st'_i を用いて r_i 、 k_i 、 s_i を生成し、 $R_i = g^{r_i}$ および $c_i = g^{k_i h(s_i)}$ を計算し、 (R_i, c_i) を鍵配送装置 S へ送信する第一鍵生成ステップと、鍵配送装置 S が、ターゲット衝突困難ハッシュ関数により $c_1, \dots, c_n$ を用いて sid を生成し、各 i について (sid, R_α, R_β) を通信装置 U_i へ送信するセッションID生成ステップと、代表通信装置 U_i が、疑似ランダム関数により $(sid, R_\alpha^{r_i})$ を用いて K_i^l を生成し、 K_i^l と $k_i || s_i$ との排他的論理和により T_i を計算し、 T_i を鍵配送装置 S へ送信する代表第二鍵生成ステップと、一般通信装置 U_j が、疑似ランダム関数により $(sid, R_\alpha^{r_j})$ を用いて K_j^l を生成し、疑似ランダム関数により $(sid, R_\beta^{r_j})$ を用いて K_j^r を生成し、 K_j^l と K_j^r との排他的論理和により T_j を計算し、 (k_j, s_j, T_j) を鍵配送装置 S へ送信する一般第二鍵生成ステップと、鍵配送装置 S が、ねじれ疑似ランダム関数により秘密ストリング st_s 、 st'_s を用いて k_s を生成し、 $k_2, \dots, k_n, k_s$ の排他的論理和により k'

を計算し、各 j について $T_1, \dots, T_{j-1}$ の排他的論理和により T'_j を計算し、 k' を代表通信装置 U_i へ送信し、 (k', T'_j, T_1) を一般通信装置 U_j へ送信する第三鍵生成ステップと、一般通信装置 U_j が、 T'_j と K_{j-1} との排他的論理和により K_j を計算し、 T_1 と K_j との排他的論理和により $k_1 || s_1$ を計算する第一セッション鍵生成ステップと、通信装置 U_i が、疑似ランダム関数により sid および k' と k_1 との排他的論理和を用いて共通鍵 K_2 を生成する第二セッション鍵生成ステップと、を含む。

発明の効果

[0009] この発明によれば、動的なメンバ変更を許しながら複数のユーザが共通鍵を共有することができる。鍵交換に必要な計算量が、ユーザ数の定数回、すなわち $O(1)$ となり、従来よりも削減されている。

図面の簡単な説明

[0010] [図1]図1は、鍵交換システムの機能構成を例示する図である。

[図2]図2(A)は、鍵配送装置の機能構成を例示する図である。図2(B)は、通信装置の機能構成を例示する図である。

[図3]図3は、鍵交換方法の処理フローを例示する図である。

[図4]図4は、鍵交換方法の処理フローを例示する図である。

発明を実施するための形態

[0011] 実施形態の説明に先立って、この明細書における表記方法について説明する。

[0012] ある集合 Set について、 Set から要素 m をランダムに選ぶことを、 $m \in_r Set$ と表記する。

[0013] あるアルゴリズム ALG について、入力 x と乱数 r に対して ALG が y を出力することを、 $y \leftarrow ALG(x; r)$ と表記する。なお、 ALG が確定的アルゴリズムの場合は、乱数 r は空である。

[0014] $|\cdot|$ は値 $\cdot$ のビット長とする。

[0015] κ をセキュリティパラメータとする。

[0016] $F = \{F_\kappa : \text{Dom}_\kappa \times \text{FS}_\kappa \rightarrow \text{Rng}_\kappa\}_\kappa$ を定義域 $\{\text{Dom}_\kappa\}_\kappa$ 、鍵空間 $\{\text{FS}_\kappa\}_\kappa$ 、値域 $\{\text{Rng}_\kappa\}_\kappa$

を持つ関数族とする。このとき、もし任意の多項式時間の識別者 D に対して、関数 F_κ と真正ランダム関数 $RF_\kappa: \text{Dom}_\kappa \rightarrow \text{Rng}_\kappa$ が見分けられなければ、 $F = \{F_\kappa\}_\kappa$ を疑似ランダム関数族と呼ぶ。疑似ランダム関数の具体例は、例えば、下記参考文献1に記載されている。

〔参考文献1〕O. ゴールドライヒ著、「現代暗号・確率的証明・疑似乱数」、シュプリンガー・フェアラク東京、2001年

[0017] $H = \{H_\kappa: \text{Dom}_\kappa \rightarrow \text{Rng}_\kappa\}_\kappa$ を定義域 $\{\text{Dom}_\kappa\}_\kappa$ 、値域 $\{\text{Rng}_\kappa\}_\kappa$ を持つハッシュ関数族とする。このとき、もし任意の多項式時間の攻撃者 A に対して、 $x \in_r \text{Dom}_\kappa$ を与えた上で $H_\kappa(x) = H_\kappa(x')$ となるような $x' (\neq x)$ を見つけられなければ、 $H = \{H_\kappa\}_\kappa$ をターゲット衝突困難ハッシュ関数族と呼ぶ。ターゲット衝突困難ハッシュ関数の具体例は、例えば、下記参考文献2に記載されている。

〔参考文献2〕J.A. ブーフマン著、「暗号理論入門 原書第3版」、丸善出版、2007年

[0018] 公開鍵暗号アルゴリズムを $(\text{Gen}, \text{Enc}, \text{Dec})$ とする。鍵生成アルゴリズム Gen はセキュリティパラメータ κ を入力とし、公開鍵 pk と秘密鍵 sk を出力する。暗号化アルゴリズム Enc は公開鍵 pk と平文 m を入力とし、暗号文 CT を出力する。復号アルゴリズム Dec は秘密鍵 sk と暗号文 CT を入力とし、平文 m を出力する。公開鍵暗号アルゴリズムの具体例は、例えば、上記参考文献2に記載されている。

[0019] メッセージ認証コードアルゴリズムを $(\text{MGen}, \text{Tag}, \text{Ver})$ とする。MAC鍵生成アルゴリズム MGen はセキュリティパラメータ κ を入力とし、MAC鍵 mk を出力する。タグ生成アルゴリズム Tag はMAC鍵 mk と平文 m を入力とし、認証タグ σ を出力する。検証アルゴリズム Ver はMAC鍵 mk と平文 m と認証タグ σ を入力とし、認証タグ σ が正しければ1を、正しくなければ0を出力する。メッセージ認証コードアルゴリズムの具体例は、例えば、上記参考文献2に記載されている。

[0020] 関数暗号アルゴリズムを $(\text{Setup}, \text{Der}, \text{FEnc}, \text{FDec})$ とする。セットアップアルゴリズム Setup はセキュリティパラメータ κ を入力とし、マスタ秘密鍵 msk と公開パラメータ Params を出力する。鍵導出アルゴリズム Der は公開パラメ

ータParamsとマスタ秘密鍵mskと属性Aを入力とし、ユーザ秘密鍵uskを出力する。暗号化アルゴリズムFEncは公開パラメータParamsとアクセス構造Pと平文mを入力とし、暗号文CTを出力する。復号アルゴリズムFDecはユーザ秘密鍵uskと暗号文CTを入力とし、属性Aがアクセス構造Pを満たすならば平文mを出力する。関数暗号アルゴリズムの具体例は、例えば、下記参考文献3に記載されている。

〔参考文献3〕 D. Boneh, A. Sahai, and B. Waters, “Functional encryption: definitions and challenges”, TCC, Lecture Notes in Computer Science, vol. 6597, pp. 253-273, 2011.

[0021] 関数tPRF: $\{0, 1\}^k \times FS_k \times \{0, 1\}^k \times FS_k \rightarrow Rng_k$ をねじれ擬似ランダム関数と呼び、擬似ランダム関数 F_k を用いて、

[数2]

$$tPRF(a, a', b, b') = F_k(a, b) \oplus F_k(b', a')$$

と定義する。ただし、 $a, b' \in \{0, 1\}^k$ であり、 $a', b \in FS_k$ である。ねじれ擬似ランダム関数の具体例は、例えば、下記参考文献4に記載されている。

〔参考文献4〕 Kazuki Yoneyama, “One-Round Authenticated Key Exchange with Strong Forward Secrecy in the Standard Model against Constrained Adversary”, IEICE Transactions, vol. E96-A, no. 6, pp. 1124-1138, 2013.

[0022] 以下、この発明の実施の形態について詳細に説明する。なお、図面中において同じ機能を有する構成部には同じ番号を付し、重複説明を省略する。

[0023] 実施形態の鍵交換システムは、図1に例示するように、鍵配送装置1およびN (≥ 2) 台の通信装置 $2_1, \dots, 2_N$ を含む。この実施形態では、鍵配送装置1および通信装置 $2_1, \dots, 2_N$ はそれぞれ通信網3へ接続される。通信網3は、鍵配送装置1が通信装置 $2_1, \dots, 2_N$ それぞれと通信可能なように構成された回線交換方式もしくはパケット交換方式の通信網である。この実施形態では、通信装置 $2_1, \dots, 2_N$ 同士は通信できなくともよい。通信網3は安全が確保された通信路である必要はなく、例えばインターネットなどを用いること

ができる。

[0024] 鍵配送装置 1 は、図 2 (A) に例示するように、記憶部 100、セットアップ部 101、公開鍵生成部 102、秘密ストリング生成部 103、ユーザ鍵送信部 111、セッションID生成部 113、認証タグ検証部 114、第三鍵生成部 115、および認証タグ生成部 116 を含む。通信装置 2 は、図 2 (B) に例示するように、記憶部 200、公開鍵生成部 202、秘密ストリング生成部 203、ユーザ鍵受信部 211、第一鍵生成部 212、第二鍵生成部 214、認証タグ生成部 215、認証タグ検証部 216、およびセッション鍵生成部 217 を含む。この鍵配送装置 1 および通信装置 2₁, ..., 2_Nが、図 3 および図 4 に例示する各ステップの処理を行うことにより実施形態の鍵交換方法が実現される。

[0025] 鍵配送装置 1 および通信装置 2₁, ..., 2_Nは、例えば、中央演算処理装置 (CPU: Central Processing Unit)、主記憶装置 (RAM: Random Access Memory) などを有する公知又は専用のコンピュータに特別なプログラムが読み込まれて構成された特別な装置である。各装置は、例えば、中央演算処理装置の制御のもとで各処理を実行する。各装置に入力されたデータや各処理で得られたデータは、例えば、主記憶装置に格納され、主記憶装置に格納されたデータは必要に応じて中央演算処理装置へ読み出されて他の処理に利用される。各装置が備える各処理部は、少なくとも一部が集積回路等のハードウェアによって構成されていてもよい。

[0026] 鍵配送装置 1 が備える記憶部 100 および通信装置 2₁, ..., 2_Nが備える記憶部 200 は、例えば、RAM (Random Access Memory) などの主記憶装置、ハードディスクや光ディスクもしくはフラッシュメモリ (Flash Memory) のような半導体メモリ素子により構成される補助記憶装置、またはリレーショナルデータベースやキーバリューストアなどのミドルウェアにより構成することができる。各記憶部は秘密情報を記憶するため、耐タンパ性を有する記憶装置 (例えば、SIMカードなど) であることが望ましい。

[0027] 図 3 を参照して、実施形態の鍵交換方法におけるシステムセットアップの

処理手続きを説明する。

- [0028] 以降の説明では、以下のように記号を定義する。Sは鍵配送装置1を示し、 U_i ($i \in \{1, \dots, N\}$)はN台の通信装置 $2_1, \dots, 2_N$ を示すものとする。Gを κ ビットの素数位数 p の乗法巡回群とする。g, hをそれぞれ群Gの生成元とする。H: $\{0, 1\}^* \rightarrow \{0, 1\}^\kappa$ をターゲット衝突困難ハッシュ関数とする。tPRF: $\{0, 1\}^\kappa \times \text{FS}_\kappa \times \{0, 1\}^\kappa \times \text{FS}_\kappa \rightarrow \mathbb{Z}_p$ 、tPRF': $\{0, 1\}^\kappa \times \text{FS}_\kappa \times \{0, 1\}^\kappa \times \text{FS}_\kappa \rightarrow \text{FS}_\kappa$ をねじれ疑似ランダム関数とする。F: $\{0, 1\}^\kappa \times G \rightarrow \mathbb{Z}_p^2$ 、F': $\{0, 1\}^\kappa \times \mathbb{Z}_p \rightarrow \text{FS}_\kappa$ 、F'': $\{0, 1\}^\kappa \times \text{FS}_\kappa \rightarrow \{0, 1\}^\kappa$ を疑似ランダム関数とする。
- [0029] ステップS101において、鍵配送装置Sのセットアップ部101は、関数暗号のセットアップアルゴリズムSetupにより公開パラメータParamsおよびマスタ秘密鍵mskを生成する。セットアップ部101は、公開パラメータParamsを通信装置 $U_1, \dots, U_N$ それぞれへ送信する。マスタ秘密鍵mskは記憶部100へ記憶される。
- [0030] ステップS102において、鍵配送装置Sの公開鍵生成部102は、公開鍵暗号の鍵生成アルゴリズムGenにより、鍵配送装置Sの公開鍵 pk_s および秘密鍵 sk_s のペアを生成する。鍵配送装置Sの公開鍵 pk_s は、例えば公開鍵基盤等を用いて公開される。鍵配送装置Sの秘密鍵 sk_s は記憶部100へ記憶される。
- [0031] ステップS202において、通信装置 U_i の公開鍵生成部202は、公開鍵暗号の鍵生成アルゴリズムGenにより、通信装置 U_i の公開鍵 pk_i および秘密鍵 sk_i のペアを生成する。通信装置 U_i の公開鍵 pk_i は、例えば公開鍵基盤等を用いて公開される。通信装置 U_i の秘密鍵 sk_i は記憶部200へ記憶される。
- [0032] ステップS103において、鍵配送装置Sの秘密ストリング生成部103は、ねじれ疑似ランダム関数で用いる秘密ストリング(st_s, st'_s)を $st_s \in \text{FS}_\kappa$ 、 $st'_s \in \{0, 1\}^\kappa$ として生成する。秘密ストリング(st_s, st'_s)は記憶部100へ記憶される。
- [0033] ステップS203において、通信装置 U_i の秘密ストリング生成部203は、ねじれ疑似ランダム関数で用いる秘密ストリング(st_i, st'_i)を $st_i \in \text{FS}_\kappa$ 、 $st'_i \in \{0, 1\}^\kappa$ として生成する。秘密ストリング(st_i, st'_i)は記憶部200へ記憶

される。

[0034] ステップS 1 0 4において、鍵配送装置Sは、各通信装置 $U_1, \dots, U_N$ の公開鍵 $pk_1, \dots, pk_N$ を例えば公開鍵基盤等から取得し、記憶部1 0 0へ記憶する。

[0035] ステップS 2 0 4において、通信装置 U_i は、鍵配送装置Sの公開鍵 pk_S を例えば公開鍵基盤等から取得し、記憶部2 0 0へ記憶する。また、鍵配送装置Sから受信した公開パラメータParamsを記憶部2 0 0へ記憶する。

[0036] 図4を参照して、実施形態の鍵交換方法におけるセッション鍵配送の処理手続きを説明する。

[0037] 以下では、N台の通信装置 $2_1, \dots, 2_N$ のうち任意の n ($\leq N$) 台の通信装置 U_i ($i \in \{1, \dots, n\}$) がセッション鍵SKの共有を行うものとする。また、 S, U_i を各アルゴリズムの入力とする場合、各装置を一意に特定する識別子を表すものとする。

[0038] ステップS 1 1 1において、鍵配送装置Sのユーザ鍵送信部1 1 1は、通信装置 U_i がセッションを開始したときに、そのセッションが通信装置 U_i のタイムフレームTFにおける最初のセッションだった場合、現在時刻をtimeとし、属性を $A_i = (U_i, \text{time})$ として、関数暗号の鍵導出アルゴリズムDerにより、通信装置 U_i のユーザ秘密鍵 $usk_i \leftarrow \text{Der}(\text{Params}, \text{msk}, A_i)$ を生成する。また、メッセージ認証コードの鍵生成アルゴリズムMGenにより、通信装置 U_i のMAC鍵 $mk_i \leftarrow \text{MGen}$ を生成する。そして、公開鍵暗号の暗号化アルゴリズムEncにより、通信装置 U_i の公開鍵 pk_i を用いてユーザ秘密鍵 usk_i およびMAC鍵 mk_i を暗号化し、暗号文 $CT_i \leftarrow \text{Enc}_{pk_i}(usk_i, mk_i)$ を生成する。ユーザ鍵送信部1 1 1は、暗号文 CT_i を通信装置 U_i へそれぞれ送信する。

[0039] ステップS 2 1 1において、通信装置 U_i のユーザ鍵受信部2 1 1は、公開鍵暗号の復号アルゴリズムDecにより、通信装置 U_i の秘密鍵 sk_i を用いて鍵配送装置Sから受信した暗号文 CT_i を復号し、ユーザ秘密鍵およびMAC鍵 $(usk_i, mk_i) \leftarrow \text{Dec}_{sk_i}(CT_i)$ を得る。ユーザ鍵受信部2 1 1は、ユーザ秘密鍵 usk_i およびMAC鍵 mk_i を記憶部2 0 0へ記憶する。

[0040] ステップS 2 1 2において、通信装置 U_i の第一鍵生成部2 1 2は、 $\tilde{r}_i \in_R \{0,$

$1\}^{\kappa}$, $\tilde{r}'_i \in {}_R\text{FS}_{\kappa}$, $\tilde{k}_i \in {}_R\{0, 1\}^{\kappa}$, $\tilde{k}'_i \in {}_R\text{FS}_{\kappa}$, $\tilde{s}_i \in {}_R\{0, 1\}^{\kappa}$, $\tilde{s}'_i \in {}_R\text{FS}_{\kappa}$ を生成し、ねじれ疑似ランダム関数tPRFにより、 $r_i = \text{tPRF}(\tilde{r}_i, \tilde{r}'_i, st_i, st'_i)$, $k_i = \text{tPRF}(\tilde{k}_i, \tilde{k}'_i, st_i, st'_i)$, $s_i = \text{tPRF}(\tilde{s}_i, \tilde{s}'_i, st_i, st'_i)$ を計算する。また、 $R_i = g^{r_i}$, $c_i = g^{k_i h^{s_i}}$ を計算する。そして、第一鍵生成部212は、 (R_i, c_i) を鍵配送装置Sへ送信する。

[0041] ステップS112において、鍵配送装置Sは、通信装置 U_i から (R_i, c_i) を受信する。このとき、すべての通信装置 $U_1, \dots, U_n$ から $(R_1, c_1), \dots, (R_n, c_n)$ を受信するまで待機する。

[0042] ステップS113において、鍵配送装置SのセッションID生成部113は、ターゲット衝突困難ハッシュ関数Hにより、通信装置 $U_1, \dots, U_n$ から受信した $c_1, \dots, c_n$ を用いて、 $sid = H(c_1, \dots, c_n)$ を生成する。また、 n 台の通信装置 $U_1, \dots, U_n$ から1台の通信装置を代表者として選択する。代表者の選択方法は任意であり、例えば、予め定めておいた優先順位が最も高い通信装置を選択してもよいし、直近でセッションを開始した通信装置を選択してもよい。ここでは、通信装置 U_1 が選択されたものとし、 U_1 を代表通信装置と呼ぶ。また、代表通信装置 U_1 以外の $n-1$ 台の通信装置 U_j ($j \in \{2, \dots, n\}$)を一般通信装置と呼ぶ。セッションID生成部113は、次式のように α, β を計算し、 $(sid, R_{\alpha}, R_{\beta})$ を通信装置 U_i へそれぞれ送信する。

[数3]

$$\alpha = \begin{cases} i-1 & \text{if } i-1 \geq 1 \\ i-1+n & \text{if } i-1 < 1 \end{cases}$$

$$\beta = \begin{cases} i+1 & \text{if } i+1 \leq n \\ i+1-n & \text{if } i+1 > n \end{cases}$$

[0043] ステップS213において、通信装置 U_i は、鍵配送装置Sから $(sid, R_{\alpha}, R_{\beta})$ をそれぞれ受信する。通信装置 U_i は、 $(sid, R_{\alpha}, R_{\beta})$ を受け取り次第、以降の処理を実行する。 $i=2, \dots, n$ の場合、すなわち通信装置 U_i が通信装置 U_j ($i=j$)であれば、ステップS214_jへ処理を進める。 $i=1$ の場合、すなわち通信装置 U_i が代表通信装置 U_1 であれば、ステップS214₁へ処理を進める。

[0044] ステップS214_jにおいて、一般通信装置 U_j の第二鍵生成部214は、次

式のように、疑似ランダム関数Fにより (sid, R_{α}^{rj}) を用いて K_j^l を生成し、疑似ランダム関数Fにより (sid, R_{β}^{rj}) を用いて K_j^r を生成し、 K_j^l と K_j^r との排他的論理和により T_j を計算する。

[数4]

$$K_j^l = F(sid, R_{\alpha}^{rj}),$$

$$K_j^r = F(sid, R_{\beta}^{rj}),$$

$$T_j = K_j^l \oplus K_j^r$$

[0045] ステップS 2 1 5_jにおいて、一般通信装置U_jの認証タグ生成部 2 1 5 は、メッセージ認証コードのタグ生成アルゴリズムTagにより、MAC鍵mk_jを用いて、認証タグ $\sigma_j = \text{Tag}_{mk_j}(R_j, c_j, R_{\alpha}, R_{\beta}, k_j, s_j, T_j, U_j, sid)$ を生成する。認証タグ生成部 2 1 5 は、 $(k_j, s_j, T_j, \sigma_j)$ を鍵配送装置Sへ送信する。

[0046] ステップS 2 1 4₁において、代表通信装置U₁の第二鍵生成部 2 1 4 は、次式のように、疑似ランダム関数Fにより (sid, R_n^{r1}) を用いて K_1^l を生成し、 K_1^l と $k_1 || s_1$ との排他的論理和により T_1 を計算する。ただし、||は連結演算子である。

[数5]

$$K_1^l = F(sid, R_n^{r1}),$$

$$T_1 = K_1^l \oplus k_1 || s_1$$

[0047] ステップS 2 1 5₁において、代表通信装置U₁の認証タグ生成部 2 1 5 は、メッセージ認証コードのタグ生成アルゴリズムTagにより、MAC鍵mk₁を用いて、認証タグ $\sigma_1 = \text{Tag}_{mk_1}(R_1, c_1, R_n, R_2, T_1, U_1, sid)$ を生成する。認証タグ生成部 2 1 5 は、 (T_1, σ_1) を鍵配送装置Sへ送信する。

[0048] ステップS 1 1 4_jにおいて、鍵配送装置Sの認証タグ検証部 1 1 4 は、j=2, ..., nについて、一般通信装置U_jから $(k_j, s_j, T_j, \sigma_j)$ を受信し、メッセージ認証コードの検証アルゴリズムVerにより、一般通信装置U_jのMAC鍵mk_jを用いて、 $\text{Ver}_{mk_j}(R_j, c_j, R_{\alpha}, R_{\beta}, k_j, s_j, T_j, U_j, sid, \sigma_j)$ を検証する。認証タグ σ_j が正当でなければ一般通信装置U_jのセッションを終了する。また、j=2, ..., nについて、 $c_j = g^{k_j h^{s_j}}$ が成り立つか否かを検証する。成り立たなければ一般通

信装置 U_j のセッションを終了する。

[0049] ステップS 1 1 4₁において、鍵配送装置Sの認証タグ検証部 1 1 4 は、代表通信装置 U_1 から (T_1, σ_1) を受信し、メッセージ認証コードの検証アルゴリズムVerにより、代表通信装置 U_1 のMAC鍵 mk_1 を用いて、 $Ver_{mk_1}(R_1, c_1, R_n, R_2, T_1, U_1, sid, \sigma_1)$ を検証する。認証タグ σ_1 が正当でなければ代表通信装置 U_1 のセッションを終了する。

[0050] ステップS 1 1 5 aにおいて、鍵配送装置Sの第三鍵生成部 1 1 5 は、 $\sim k_s \in_R \{0, 1\}^K$, $\sim k'_s \in_R FS_K$, $\sim K_1 \in_R \{0, 1\}^K$, $\sim K'_1 \in_R FS_K$ を生成し、ねじれ疑似ランダム関数tPRFにより、 $k_s = tPRF(\sim k_s, \sim k'_s, st_s, st'_s)$, $K_1 = tPRF(\sim K_1, \sim K'_1, st_s, st'_s)$ を計算する。また、次式により、 k' を計算する。

[数6]

$$k' = (\oplus_{2 \leq j \leq n} k_j) \oplus k_s$$

[0051] ステップS 1 1 5 bにおいて、鍵配送装置Sの第三鍵生成部 1 1 5 は、 $j=2, \dots, n$ について、次式により、 T'_j を計算する。

[数7]

$$T'_j = \oplus_{1 \leq i \leq j-1} T_i$$

[0052] ステップS 1 1 5 cにおいて、鍵配送装置Sの第三鍵生成部 1 1 5 は、 $i=1, \dots, n$ について、アクセス構造 $P_i = (ID=U_i) \wedge (time \in TF)$ として、関数暗号の暗号化アルゴリズムFEncにより共通鍵 K_1 を暗号化して、暗号文 $CT'_i = FEnc(Params, P_i, K_1)$ を生成する。ここで、IDは通信装置を表す述語変数であり、TFは通信装置のタイムフレームを表す述語変数である。

[0053] ステップS 1 1 6_jにおいて、鍵配送装置Sの認証タグ生成部 1 1 6 は、 $j=2, \dots, n$ について、メッセージ認証コードのタグ生成アルゴリズムTagにより、一般通信装置 U_j のMAC鍵 mk_j を用いて認証タグ $\sigma'_j = Tag_{mk_j}(R_j, c_j, R_\alpha, R_\beta, k_j, s_j, T_j, U_j, sid, c_1, k', T'_j, T_1, CT'_j)$ を生成する。認証タグ生成部 1 1 6 は、 $(c_1, k', T'_j, T_1, CT'_j, \sigma'_j)$ を一般通信装置 U_j へ送信する。

[0054] ステップS 1 1 6₁において、鍵配送装置Sの認証タグ生成部 1 1 6 は、メッセージ認証コードのタグ生成アルゴリズムTagにより、代表通信装置 U_1 のMAC鍵

mk_1 を用いて、認証タグ $\sigma'_1 = \text{Tag}_{mk_1}(R_1, c_1, R_n, R_2, T_1, U_1, \text{sid}, k', CT'_1)$ を生成する。認証タグ生成部 116 は、 (k', CT'_1, σ'_1) を代表通信装置 U_1 へ送信する。

- [0055] ステップS 216_jにおいて、一般通信装置 U_j の認証タグ検証部 216 は、鍵配送装置Sから $(c_1, k', T'_j, T_1, CT'_j, \sigma'_j)$ を受信し、メッセージ認証コードの検証アルゴリズムVerにより、一般通信装置 U_j のMAC鍵 mk_j を用いて、 $\text{Ver}_{mk_j}(R_j, c_j, R_\alpha, R_\beta, k_j, s_j, T_j, U_j, \text{sid}, c_1, k', T'_j, T_1, CT'_j, \sigma'_j)$ を検証する。認証タグ σ'_j が正当でなければ一般通信装置 U_j のセッションを終了する。また、次式のように、 T'_j と K_j^l との排他的論理和により K_j^l を計算し、 T_1 と K_j^l との排他的論理和により $k_1 \parallel s_1$ を計算する。

[数8]

$$K_1^l = T'_j \oplus K_j^l,$$

$$k_1 \parallel s_1 = T_1 \oplus K_1^l$$

- [0056] そして、 $c_1 = g^{k_1} h^{s_1}$ が成り立つか否かを検証する。成り立たなければ一般通信装置 U_j のセッションを終了する。

- [0057] ステップS 216₁において、代表通信装置 U_1 の認証タグ検証部 216 は、鍵配送装置Sから (k', CT'_1, σ'_1) を受信し、メッセージ認証コードの検証アルゴリズムVerにより、代表通信装置 U_1 のMAC鍵 mk_1 を用いて、 $\text{Ver}_{mk_1}(R_1, c_1, R_n, R_2, T_1, U_1, \text{sid}, k', CT'_1, \sigma'_1)$ を検証する。認証タグ σ'_1 が正当でなければ代表通信装置 U_1 のセッションを終了する。

- [0058] ステップS 217において、通信装置 U_i のセッション鍵生成部 217 は、関数暗号の復号アルゴリズムFDecにより、通信装置 U_i のユーザ秘密鍵 usk_i を用いて、共通鍵 $K_1 \leftarrow \text{FDec}_{usk_i}(CT'_i, P_i)$ を復号する。また、次式のように、疑似ランダム関数 F' により共通鍵 K_2 を計算する。

[数9]

$$K_2 = F'(\text{sid}, k' \oplus k_1)$$

- [0059] そして、次式のように、疑似ランダム関数 F'' によりセッション鍵SKを計算する。

[数10]

$$SK = F^*(sid, K_1) \oplus F^*(sid, K_2)$$

[0060] 上記のように構成することにより、この発明の鍵交換技術によれば、従来のように事前に鍵交換を行うユーザの情報を登録しておく必要がなく、動的なメンバ変更を許しながら複数のユーザが共通鍵を共有することができる。また、従来は鍵交換に必要な全体の計算量がユーザ数を n として $O(\log n)$ となるが、この発明によればユーザ数の定数回、すなわち $O(1)$ となるため、従来よりも少ない計算量で鍵交換ができる。

[0061] この発明は上述の実施形態に限定されるものではなく、この発明の趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。上記実施形態において説明した各種の処理は、記載の順に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

[0062] [プログラム、記録媒体]

上記実施形態で説明した各装置における各種の処理機能をコンピュータによって実現する場合、各装置が有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムをコンピュータで実行することにより、上記各装置における各種の処理機能がコンピュータ上で実現される。

[0063] この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等のようなものでもよい。

[0064] また、このプログラムの流通は、例えば、そのプログラムを記録したDVD、CD-ROM等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

[0065] このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理の実行時、このコンピュータは、自己の記録媒体に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。また、サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるASP (Application Service Provider) 型のサービスによって、上述の処理を実行する構成としてもよい。なお、本形態におけるプログラムには、電子計算機による処理の用に供する情報であってプログラムに準ずるもの（コンピュータに対する直接の指令ではないがコンピュータの処理を規定する性質を有するデータ等）を含むものとする。

[0066] また、この形態では、コンピュータ上で所定のプログラムを実行させることにより、本装置を構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

請求の範囲

[請求項1] n を2以上の整数とし、 i を1から n までの各整数とし、 j を2から n までの各整数とし、 S を鍵配送装置とし、 U_i を n 台の通信装置とし、 U_i を上記通信装置 U_i から選択された1台の代表通信装置とし、 U_j を上記通信装置 U_i から上記代表通信装置 U_i を除いた $n-1$ 台の一般通信装置とし、 $||$ を連結演算子とし、 α 、 β を次式で定義される整数とし、

[数11]

$$\alpha = \begin{cases} i-1 & \text{if } i-1 \geq 1 \\ i-1+n & \text{if } i-1 < 1 \end{cases}$$

$$\beta = \begin{cases} i+1 & \text{if } i+1 \leq n \\ i+1-n & \text{if } i+1 > n \end{cases}$$

上記鍵配送装置 S の記憶部に、上記鍵配送装置 S の公開鍵暗号の秘密鍵 sk_s および秘密ストリング st_s 、 st'_s が記憶されており、

上記通信装置 U_i の記憶部に、上記通信装置 U_i の公開鍵暗号の秘密鍵 k_i および秘密ストリング st_i 、 st'_i が記憶されており、

上記通信装置 U_i が、ねじれ疑似ランダム関数により上記秘密ストリング st_i 、 st'_i を用いて r_i 、 k_i 、 s_i を生成し、 $R_i = g^{r_i}$ および $c_i = g^{k_i h^{s_i}}$ を計算し、 (R_i, c_i) を上記鍵配送装置 S へ送信する第一鍵生成ステップと、

上記鍵配送装置 S が、ターゲット衝突困難ハッシュ関数により $c_1, \dots, c_n$ を用いて sid を生成し、各 i について (sid, R_α, R_β) を上記通信装置 U_i へ送信するセッションID生成ステップと、

上記代表通信装置 U_i が、疑似ランダム関数により $(sid, R_\alpha^{r_i})$ を用いて K_i^l を生成し、 K_i^l と $k_i || s_i$ との排他的論理和により T_i を計算し、 T_i を上記鍵配送装置 S へ送信する代表第二鍵生成ステップと、

上記一般通信装置 U_j が、疑似ランダム関数により $(sid, R_\alpha^{r_j})$ を用いて K_j^l を生成し、疑似ランダム関数により $(sid, R_\beta^{r_j})$ を用いて K_j^r を生成し、 K_j^l と K_j^r との排他的論理和により T_j を計算し、 (k_j, s_j, T_j) を上記鍵配送装置 S へ送信する一般第二鍵生成ステップと、

上記鍵配送装置 S が、ねじれ疑似ランダム関数により上記秘密スト

リング st_s, st'_s を用いて k_s を生成し、 $k_2, \dots, k_n, k_s$ の排他的論理和により k' を計算し、各 j について $T_1, \dots, T_{j-1}$ の排他的論理和により T'_j を計算し、 k' を上記代表通信装置 U_1 へ送信し、 (k', T'_j, T_1) を上記一般通信装置 U_j へ送信する第三鍵生成ステップと、

上記一般通信装置 U_j が、 T'_j と K_j^r との排他的論理和により K_j^l を計算し、 T_1 と K_j^l との排他的論理和により $k_1 || s_1$ を計算する第一セッション鍵生成ステップと、

上記通信装置 U_i が、疑似ランダム関数により sid および k' と k_1 との排他的論理和を用いて共通鍵 K_2 を生成する第二セッション鍵生成ステップと、

を含む鍵交換方法。

[請求項2]

請求項1に記載の鍵交換方法であって、

$time$ を現在時刻とし、 ID を上記通信装置を表す述語変数とし、 TF を上記通信装置のタイムフレームを表す述語変数とし、

上記鍵配送装置 S の記憶部に、関数暗号のマスタ秘密鍵 msk がさらに記憶されており、

上記鍵配送装置 S が、各 i について属性を $A_i=(U_i, time)$ として関数暗号の鍵導出アルゴリズムにより上記マスタ秘密鍵 msk を用いてユーザ秘密鍵 usk_i を生成し、公開鍵暗号の暗号化アルゴリズムにより上記通信装置 U_i の公開鍵 pk_i を用いて上記ユーザ秘密鍵 usk_i を暗号化して暗号文 CT_i を生成するユーザ鍵送信ステップと、

上記通信装置 U_i が、公開鍵暗号の復号アルゴリズムにより上記秘密鍵 sk_i を用いて上記暗号文 CT_i を復号して上記ユーザ秘密鍵 usk_i を得るユーザ鍵受信ステップと、

をさらに含み、

上記第三鍵生成ステップは、ねじれ疑似ランダム関数により上記秘密ストリング st_s, st'_s を用いて共通鍵 K_1 を生成し、各 i についてアクセス構造を $P_i=(ID=U_i) \wedge (time \in TF)$ として関数暗号の暗号化アルゴリ

ズムにより上記共通鍵 K_1 を暗号化して暗号文 CT'_i を生成するものであり、

上記第二セッション鍵生成ステップは、関数暗号の復号アルゴリズムにより上記ユーザ秘密鍵 usk_i を用いて上記暗号文 CT'_i を復号して上記共通鍵 K_1 を得、疑似ランダム関数により (sid, K_1) を用いて生成した値と疑似ランダム関数により (sid, K_2) を用いて生成した値との排他的論理和によりセッション鍵 SK を計算するものである、

鍵交換方法。

[請求項3]

請求項2に記載の鍵交換方法であって、

上記ユーザ鍵送信ステップは、メッセージ認証コードの鍵生成アルゴリズムによりMAC鍵 mk_i を生成し、公開鍵暗号の暗号化アルゴリズムにより上記通信装置 U_i の公開鍵 pk_i を用いて上記ユーザ秘密鍵 usk_i および上記MAC鍵 mk_i を暗号化して上記暗号文 CT_i を生成するものであり、

上記ユーザ鍵受信ステップは、公開鍵暗号の復号アルゴリズムにより上記秘密鍵 sk_i を用いて上記暗号文 CT_i を復号して上記ユーザ秘密鍵 usk_i および上記MAC鍵 mk_i を得るものであり、

上記代表通信装置 U_1 が、メッセージ認証コードのタグ生成アルゴリズムにより上記MAC鍵 mk_1 および $R_1, c_1, R_n, R_2, T_1, U_1, sid$ を用いて認証タグ σ_1 を生成する代表第一認証タグ生成ステップと、

上記一般通信装置 U_j が、メッセージ認証コードのタグ生成アルゴリズムにより上記MAC鍵 mk_j および $R_j, c_j, R_\alpha, R_\beta, k_j, s_j, T_j, U_j, sid$ を用いて認証タグ σ_j を生成する一般第一認証タグ生成ステップと、

上記鍵配送装置 S が、メッセージ認証コードの検証アルゴリズムにより上記MAC鍵 mk_1 および $R_1, c_1, R_n, R_2, T_1, U_1, sid$ を用いて上記認証タグ σ_1 を検証し、各 j についてメッセージ認証コードの検証アルゴリズムにより上記MAC鍵 mk_j および $R_j, c_j, R_\alpha, R_\beta, k_j, s_j, T_j, U_j, sid$ を用いて上記認証タグ σ_j を検証し、 $c_j = g^{k_j} h^{s_j}$ が成り立つか否かを検証する第一認証タグ検証ステップと、

上記鍵配送装置Sが、メッセージ認証コードのタグ生成アルゴリズムにより上記MAC鍵 mk_1 および $R_1, c_1, R_n, R_2, T_1, U_1, sid, k', CT'_1$ を用いて認証タグ σ'_1 を生成し、各jについてメッセージ認証コードのタグ生成アルゴリズムにより上記MAC鍵 mk_j および $R_j, c_j, R_\alpha, R_\beta, k_j, s_j, T_j, U_j, sid, c_1, k', T'_j, T_1, CT'_j$ を用いて認証タグ σ'_j を生成する第二認証タグ生成ステップと、

上記代表通信装置 U_1 が、メッセージ認証コードの検証アルゴリズムにより上記MAC鍵 mk_1 および $R_1, c_1, R_n, R_2, T_1, U_1, sid, k', CT'_1$ を用いて上記認証タグ σ'_1 を検証する代表第二認証タグ検証ステップと、

上記一般通信装置 U_j が、メッセージ認証コードの検証アルゴリズムにより上記MAC鍵 mk_j および $R_j, c_j, R_\alpha, R_\beta, k_j, s_j, T_j, U_j, sid, c_1, k', T'_j, T_1, CT'_j$ を用いて上記認証タグ σ'_j を検証し、 T'_j と K_j^{-1} との排他的論理和により K_j^{-1} を計算し、 T_1 と K_j^{-1} との排他的論理和により $k_1 || s_1$ を求め、 $c_1 = g^{k_1} h^{s_1}$ が成り立つか否かを検証する一般第二認証タグ検証ステップと、

をさらに含む鍵交換方法。

[請求項4]

n を2以上の整数とし、 i を1から n までの各整数とし、 j を2から n までの各整数とし、 $||$ を連結演算子とし、 α, β を次式で定義される整数とし、

[数12]

$$\alpha = \begin{cases} i-1 & \text{if } i-1 \geq 1 \\ i-1+n & \text{if } i-1 < 1 \end{cases}$$

$$\beta = \begin{cases} i+1 & \text{if } i+1 \leq n \\ i+1-n & \text{if } i+1 > n \end{cases}$$

鍵配送装置Sと n 台の通信装置 U_i とを含み、上記通信装置 U_i は代表通信装置 U_1 と $n-1$ 台の一般通信装置 U_j とからなる鍵交換システムであって、

上記鍵配送装置Sは、

上記鍵配送装置Sの公開鍵暗号の秘密鍵 sk_s および秘密ストリング

st_s , st'_s を記憶する記憶部と、

各 i について上記通信装置 U_i から (R_i, c_i) を受信し、ターゲット衝突困難ハッシュ関数により $c_1, \dots, c_n$ を用いて sid を生成し、各 i について (sid, R_α, R_β) を上記通信装置 U_i へ送信するセッションID生成部と、

上記代表通信装置 U_1 から T_1 を受信し、各 j について上記一般通信装置 U_j から (k_j, s_j, T_j) を受信し、ねじれ疑似ランダム関数により上記秘密ストリング st_s , st'_s を用いて k_s を生成し、 $k_2, \dots, k_n$, k_s の排他的論理和により k' を計算し、各 j について $T_1, \dots, T_{j-1}$ の排他的論理和により T'_j を計算し、 k' を上記代表通信装置 U_1 へ送信し、 (k', T'_j, T_1) を上記一般通信装置 U_j へ送信する第三鍵生成部と、

を含み、

上記代表通信装置 U_1 は、

上記代表通信装置 U_1 の公開鍵暗号の秘密鍵 sk_1 および秘密ストリング st_1 , st'_1 を記憶する記憶部と、

ねじれ疑似ランダム関数により上記秘密ストリング st_1 , st'_1 を用いて r_1 , k_1 , s_1 を生成し、 $R_1 = g^{r_1}$ および $c_1 = g^{k_1} h^{s_1}$ を計算し、 (R_1, c_1) を上記鍵配送装置 S へ送信する第一鍵生成部と、

上記鍵配送装置 S から (sid, R_n, R_2) を受信し、疑似ランダム関数により $(sid, R_n^{r_1})$ を用いて $K_1^{r_1}$ を生成し、 $K_1^{r_1}$ と $k_1 || s_1$ との排他的論理和により T_1 を計算し、 T_1 を上記鍵配送装置 S へ送信する第二鍵生成部と、

上記鍵配送装置 S から k' を受信し、疑似ランダム関数により sid および k' と k_1 との排他的論理和を用いて共通鍵 K_2 を生成するセッション鍵生成部と、

を含み、

上記一般通信装置 U_j は、

上記一般通信装置 U_j の公開鍵暗号の秘密鍵 sk_j および秘密ストリング st_j , st'_j を記憶する記憶部と、

ねじれ疑似ランダム関数により上記秘密ストリング st_j , st'_j を用いて r_j , k_j , s_j を生成し、 $R_j=g^{r_j}$ および $c_j=g^{k_j}h^{s_j}$ を計算し、 (R_j, c_j) を上記鍵配送装置Sへ送信する第一鍵生成部と、

上記鍵配送装置Sから (sid, R_α, R_β) を受信し、疑似ランダム関数により $(sid, R_\alpha^{r_j})$ を用いて K_j^l を生成し、疑似ランダム関数により $(sid, R_\beta^{r_j})$ を用いて K_j^r を生成し、 K_j^l と K_j^r との排他的論理和により T_j を計算し、 (k_j, s_j, T_j) を上記鍵配送装置Sへ送信する第二鍵生成部と、

上記鍵配送装置Sから (k', T'_j, T_1) を受信し、 T'_j と K_j^r との排他的論理和により K_j^l を計算し、 T_1 と K_j^l との排他的論理和により $k_1 || s_1$ を計算し、疑似ランダム関数により sid および k' と k_1 との排他的論理和を用いて上記共通鍵 K_2 を生成するセッション鍵生成部と、

を含む鍵交換システム。

[請求項5] n を2以上の整数とし、 i を1から n までの各整数とし、 j を2から n までの各整数とし、 α , β を次式で定義される整数とし、

[数13]

$$\alpha = \begin{cases} i-1 & \text{if } i-1 \geq 1 \\ i-1+n & \text{if } i-1 < 1 \end{cases}$$

$$\beta = \begin{cases} i+1 & \text{if } i+1 \leq n \\ i+1-n & \text{if } i+1 > n \end{cases}$$

公開鍵暗号の秘密鍵 sk_s および秘密ストリング st_s , st'_s を記憶する記憶部と、

各 i について通信装置 U_i から (R_i, c_i) を受信し、ターゲット衝突困難ハッシュ関数により $c_1, \dots, c_n$ を用いて sid を生成し、各 i について (sid, R_α, R_β) を上記通信装置 U_i へ送信するセッションID生成部と、

代表通信装置 U_1 から T_1 を受信し、各 j について一般通信装置 U_j から (k_j, s_j, T_j) を受信し、ねじれ疑似ランダム関数により上記秘密ストリング st_s , st'_s を用いて k_s を生成し、 $k_2, \dots, k_n$, k_s の排他的論理和により k' を計算し、各 j について $T_1, \dots, T_{j-1}$ の排他的論理和により T'_j を計算し、 k' を上記代表通信装置 U_1 へ送信し、 (k', T'_j, T_1) を上記一般

通信装置 U_j へ送信する第三鍵生成部と、

を含む鍵配送装置。

[請求項6]

n を2以上の整数とし、 $||$ を連結演算子とし、

公開鍵暗号の秘密鍵 sk_1 および秘密ストリング st_1 , st'_1 を記憶する記憶部と、

ねじれ疑似ランダム関数により上記秘密ストリング st_1 , st'_1 を用いて r_1 , k_1 , s_1 を生成し、 $R_1=g^{r_1}$ および $c_1=g^{k_1}h^{s_1}$ を計算し、 (R_1, c_1) を鍵配送装置 S へ送信する第一鍵生成部と、

上記鍵配送装置 S から (sid, R_n, R_2) を受信し、疑似ランダム関数により $(sid, R_n^{r_1})$ を用いて K_1^l を生成し、 K_1^l と $k_1||s_1$ との排他的論理和により T_1 を計算し、 T_1 を上記鍵配送装置 S へ送信する第二鍵生成部と、

上記鍵配送装置 S から k' を受信し、疑似ランダム関数により sid および k' と k_1 との排他的論理和を用いて共通鍵 K_2 を生成するセッション鍵生成部と、

を含む通信装置。

[請求項7]

n を2以上の整数とし、 j を2以上 n 以下の整数とし、 $||$ を連結演算子とし、 α , β を次式で定義される整数とし、

[数14]

$$\alpha = \begin{cases} j-1 & \text{if } j-1 \geq 1 \\ j-1+n & \text{if } j-1 < 1 \end{cases}$$

$$\beta = \begin{cases} j+1 & \text{if } j+1 \leq n \\ j+1-n & \text{if } j+1 > n \end{cases}$$

公開鍵暗号の秘密鍵 sk_j および秘密ストリング st_j , st'_j を記憶する記憶部と、

ねじれ疑似ランダム関数により上記秘密ストリング st_j , st'_j を用いて r_j , k_j , s_j を生成し、 $R_j=g^{r_j}$ および $c_j=g^{k_j}h^{s_j}$ を計算し、 (R_j, c_j) を鍵配送装置 S へ送信する第一鍵生成部と、

上記鍵配送装置 S から (sid, R_α, R_β) を受信し、疑似ランダム関数により $(sid, R_\alpha^{r_j})$ を用いて K_j^l を生成し、疑似ランダム関数により $(si$

$d, R_{\beta}^{rj})$ を用いて K_j^r を生成し、 K_j^l と K_j^r との排他的論理和により T_j を計算し、 (k_j, s_j, T_j) を上記鍵配送装置Sへ送信する第二鍵生成部と、

上記鍵配送装置Sから (k', T'_j, T_1) を受信し、 T'_j と K_j^r との排他的論理和により K_j^l を計算し、 T_1 と K_j^l との排他的論理和により $k_1 || s_1$ を計算し、疑似ランダム関数によりsidおよび k' と k_1 との排他的論理和を用いて共通鍵 K_2 を生成するセッション鍵生成部と、

を含む通信装置。

[請求項8] 請求項5に記載の鍵配送装置もしくは請求項6または7に記載の通信装置としてコンピュータを機能させるためのプログラム。

[図1]

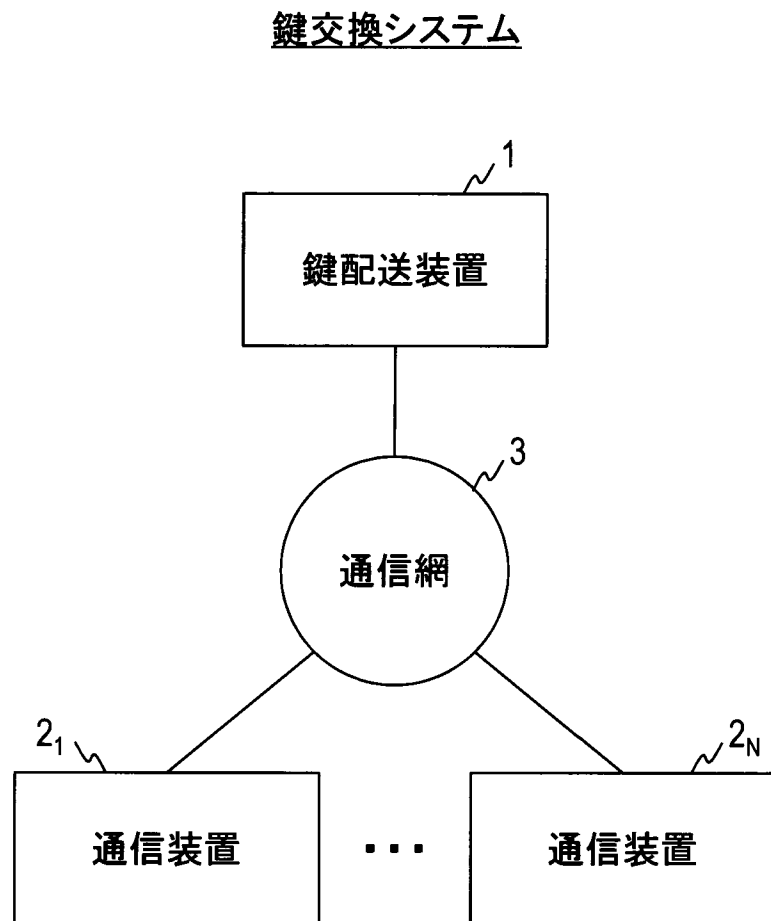


図1

[図2]

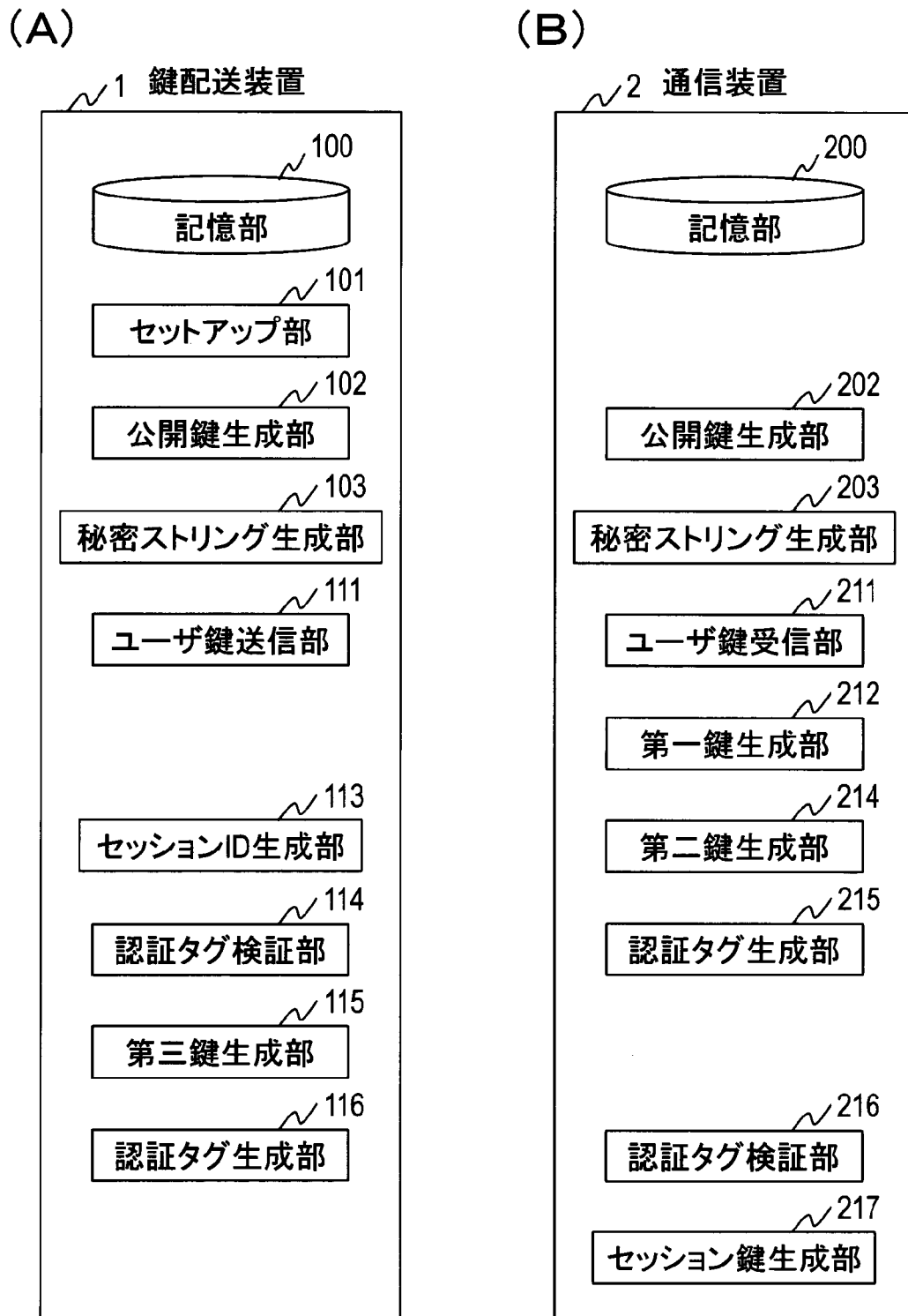


図2

[図3]

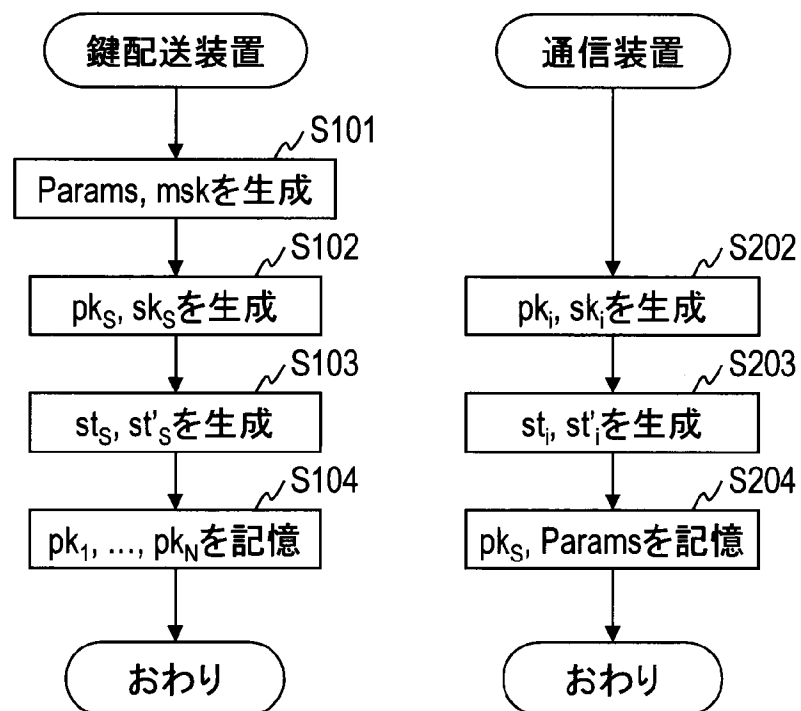


図3

[図4]

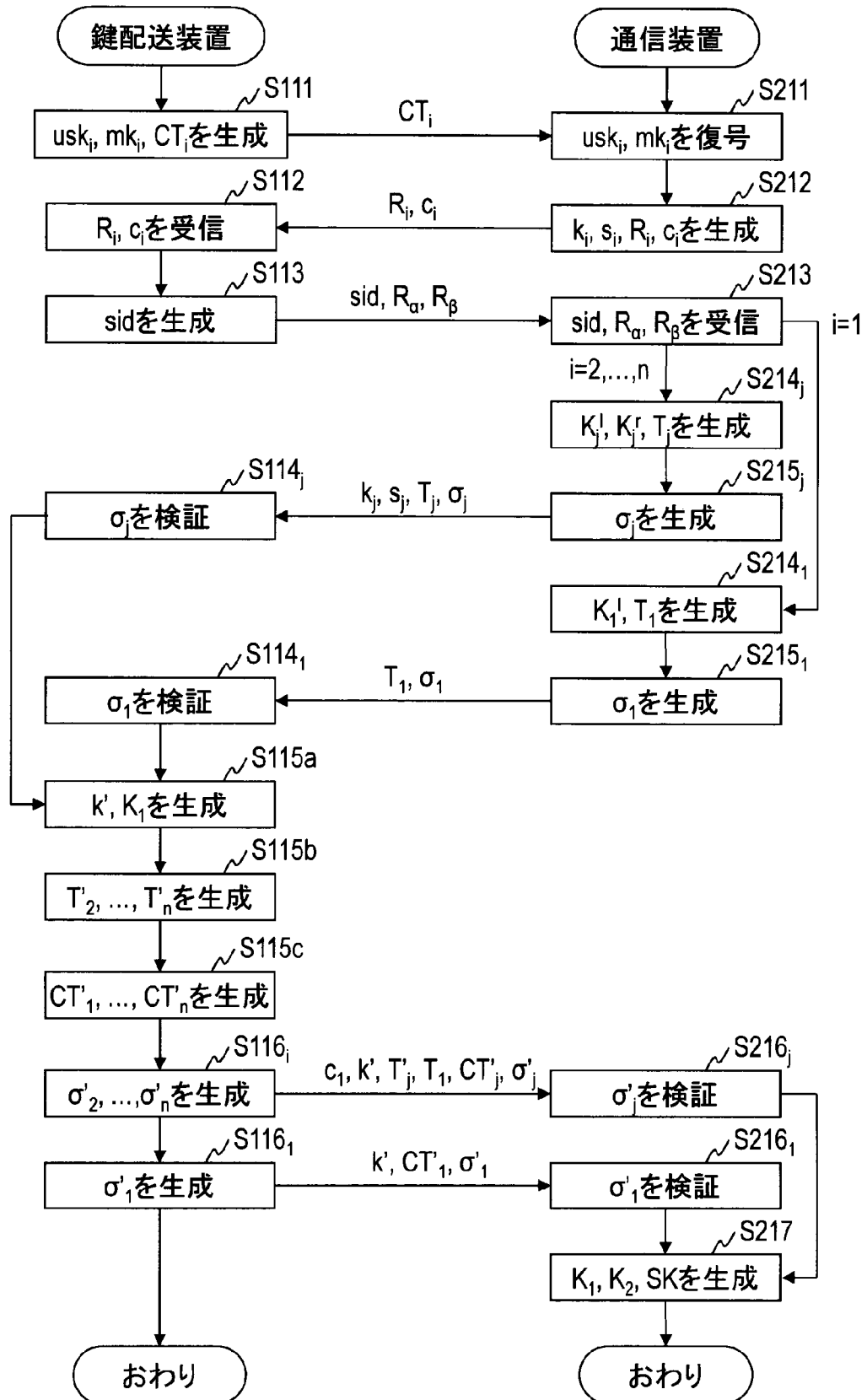


図4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/062601

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01)i, H04L9/32(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)

H04L9/08, H04L9/32

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	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JUNG, Bae Eun, An Efficient Group Key Agreement Protocol, IEEE Communications Letters, 2006.02, Vol. 10, No. 2, pp. 106-107	1-8
A	JP 2006-245663 A (Matsushita Electric Industrial Co., Ltd.), 14 September 2006 (14.09.2006), (Family: none)	1-8
T	KOBAYASHI, Tetsutaro et al., Scalable and Dynamic Multi-Cast Key Distribution, 2016 Symposium on Cryptography and Information Security, 2016.01.19, 4E2-3	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

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
08 July 2016 (08.07.16)

Date of mailing of the international search report
19 July 2016 (19.07.16)

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, H04L9/32(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, H04L9/32

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	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016年

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

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JUNG, Bae Eun, An Efficient Group Key Agreement Protocol, IEEE Communications Letters, 2006.02, Vol. 10, No. 2, pp. 106-107	1-8
A	JP 2006-245663 A（松下電器産業株式会社）2006.09.14 （ファミリーなし）	1-8
T	KOBAYASHI, Tetsutaro et al., Scalable and Dynamic Multi-Cast Key Distribution, 2016 Symposium on Cryptography and Information Security, 2016.01.19, 4E2-3	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
「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

08.07.2016

国際調査報告の発送日

19.07.2016

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）

金沢 史明

5 S

4538

電話番号 03-3581-1101 内線 3546