(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
2006 年3 月16 日 (16.03.2006)

PCT

(10) 国際公開番号
WO 2006/027933 A1

(51) 国際特許分類:
H04L 9/32 (2006.01)

(21) 国際出願番号: PCT/JP2005/014783

(22) 国際出願日: 2005 年8 月11 日 (11.08.2005)

(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2004-257660 2004 年9 月3 日 (03.09.2004) 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): 米澤 祥子 (YONEZAWA, Shoko) [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). 佐古 和恵 (SAKO, Kazue) [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).

(74) 代理人: 丸山 隆夫 (MARUYAMA, Takao); 〒1700013 東京都豊島区東池袋２－３８－２３ ＳＡＭビル ３階 丸山特許事務所 Tokyo (JP).

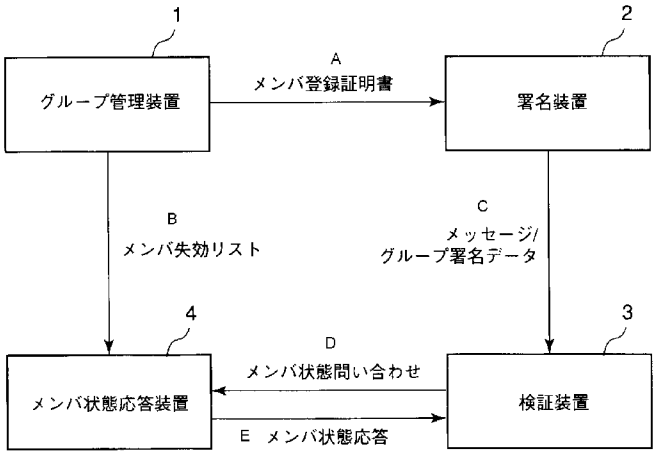
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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,

[続葉有]

(54) **Title:** GROUP SIGNATURE SYSTEM, MEMBER STATE JUDGMENT DEVICE, GROUP SIGNATURE METHOD, AND MEMBER STATE JUDGMENT PROGRAM

(54) 発明の名称: グループ署名システム、メンバ状態判定装置、グループ署名方法及びメンバ状態判定プログラム



1... GROUP MANAGEMENT DEVICE
2... SIGNATURE DEVICE
3... VERIFICATION DEVICE
4... MEMBER STATE RESPONSE DEVICE
A... MEMBER REGISTRATION CERTIFICATE
B... MEMBER INVALIDATION LIST
C... MESSAGE/GROUP SIGNATURE DATA
D... MEMBER STATE INQUIRY
E... MEMBER STATE RESPONSE

(57) **Abstract:** Concerning group signature data capable of keeping anonymity, it is possible to effectively judge whether the user who has generated the group signature data is a valid member of the group. Upon reception of a message and group signature data, a verification device (3) authenticates the group signature data and asks a member state response device (4) whether the user of the signature device Z (2) who has generated the group signature data is a valid member of the group. In response to the inquiry, the member state response device (4) judges the member state of the user of the signature device (2) who has generated the group signature data according to a member invalidation list reported from a group management device (1). The member state response device (4) transmits the judgment result of the member state to the verification device (3).

(57) 要約: 匿名性を保つことが可能なグループ署名データに対して、グループ署名データを生成したユーザがグループの有効なメンバであるか否かを効率的に判定できるようにする。 検証装置３は、メッセージとグループ署名データとを受け取ると、

[続葉有]

WO 2006/027933 A1

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, HU, IE, IS, IT, LT, LU, LV, MC, NL, 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

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

グループ署名データを認証するとともに、グループ署名データを生成した署名装置２のユーザがグループの有効なメンバであるか否かをメンバ状態応答装置４に問い合わせる。メンバ状態応答装置４は、問い合わせに応じて、グループ管理装置１から通知されたメンバ失効リストにもとづいて、グループ署名データを生成した署名装置２のユーザのメンバ状態を判定する。そして、メンバ状態応答装置４は、検証装置３にメンバ状態の判定結果を送信する。