(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8 月17 日 (17.08.2006)

PCT

(10) 国際公開番号
WO 2006/085430 A1

(51) 国際特許分類:
H04L 9/32 (2006.01)

(21) 国際出願番号: PCT/JP2006/300428

(22) 国際出願日: 2006 年1 月16 日 (16.01.2006)

(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2005-034961 2005 年2 月10 日 (10.02.2005) 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).

(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, 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, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, 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.

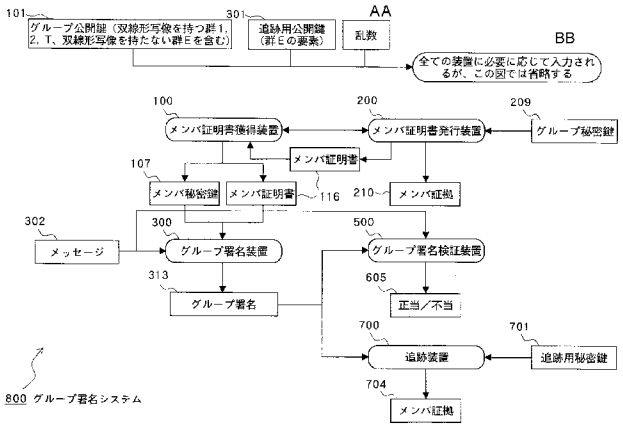
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

[続葉有]

(54) **Title:** MEMBER CERTIFICATE ACQUIRING DEVICE, MEMBER CERTIFICATE ISSUING DEVICE, GROUP SIGNING DEVICE, AND GROUP SIGNATURE VERIFYING DEVICE

(54) 発明の名称: メンバー証明書獲得装置、メンバー証明書発行装置、グループ署名装置、グループ署名検証装置



101 GROUP PUBLIC KEY (CONTAINING GROUP 1, GROUP 2, GROUP T HAVING BILINEAR MAPPING AND GROUP E NOT HAVING BILINEAR MAPPING)
301 TRACKING PUBLIC KEY (ELEMENT OF GROUP E)
AA RANDOM NUMBER
BB THESE ARE INPUTTED INTO ALL DEVICES AS NECESSARY, BUT INPUT ARE NOT SHOWN IN THIS DRAWING
100 MEMBER CERTIFICATE ACQUIRING DEVICE
200 MEMBER CERTIFICATE ISSUING DEVICE
209 GROUP SECRET KEY
116 MEMBER CERTIFICATE
107 MEMBER SECRET KEY
800 GROUP SIGNING SYSTEM
704 MEMBER EVIDENCE
300 GROUP SIGNING DEVICE
313 GROUP SIGNATURE
500 GROUP SIGNATURE VERIFYING DEVICE
605 AUTHENTICATED/NONAUTHENTICATED
700 TRACKING DEVICE
701 TRACKING SECRET KEY
210 MEMBER EVIDENCE
302 MESSAGE

(57) **Abstract:** The security of a group signature system is improved, and the amount of data handled is reduced. when a group public key containing description of four groups, i.e., group 1, group 2, group T, and group E having the same order, description of a bilinear mapping from groups 1, 2, to group T, the generator of group 1, group 2, group T, and group E, and a signature public key of a singing method using group 1, group 2, and group T, a member secret key containing an integer equal to or smaller than the order, a member evidence which is the product of the generator of group E multiplied by the

[続葉有]

WO 2006/085430 A1

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。

member secret key, and the element of group 1 or 2 which is the product of the generator of group 1 or 2 multiplied by the member secret key are sent to the member certificate issuing device. Thereafter, when a signature for the member secret key verifiable with the signature public key is received from the member certificate issuing device, the signature is used as the member certificate.

(57) 要約:　本発明は、グループ署名システムにおける安全性を向上し、また、扱うデータ量を低減することを目的とし、位数が同じである群１、群２、群Ｔ、群Ｅの４個の群に対する記述と、群１と群２から群Ｔへの双線形写像の記述と、群１、群２、群Ｔ、群Ｅの各生成子と、前記群１、前記群２、前記群Ｔを用いた署名方式の署名公開鍵とが含まれる前記グループ公開鍵が入力されると、前記位数以下の整数を含む前記メンバ秘密鍵と、前記群Ｅの前記生成子に前記メンバ秘密鍵を乗じた値であるメンバ証拠と、前記群１あるいは群２の前記生成子に前記メンバ秘密鍵を乗じた値である前記群１あるいは群２の要素と、を前記メンバ証明書発行装置に送信し、その後、前記メンバ証明書発行装置より前記署名公開鍵で検証可能な、前記メンバ秘密鍵に対する署名を受信すると、該署名を前記メンバ証明書とする。