(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
2005 年8 月4 日 (04.08.2005)

PCT

(10) 国際公開番号
WO 2005/071881 A1

(51) 国際特許分類[7]: H04L 9/32

(21) 国際出願番号: PCT/JP2005/000841

(22) 国際出願日: 2005 年1 月24 日 (24.01.2005)

(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2004-014560 2004 年1 月22 日 (22.01.2004) 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): 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). 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: 山川 政樹, 外(YAMAKAWA, Masaki et al.); 〒1000014 東京都千代田区永田町２丁目４番２号 秀和溜池ビル８階 山川国際特許事務所内 Tokyo (JP).

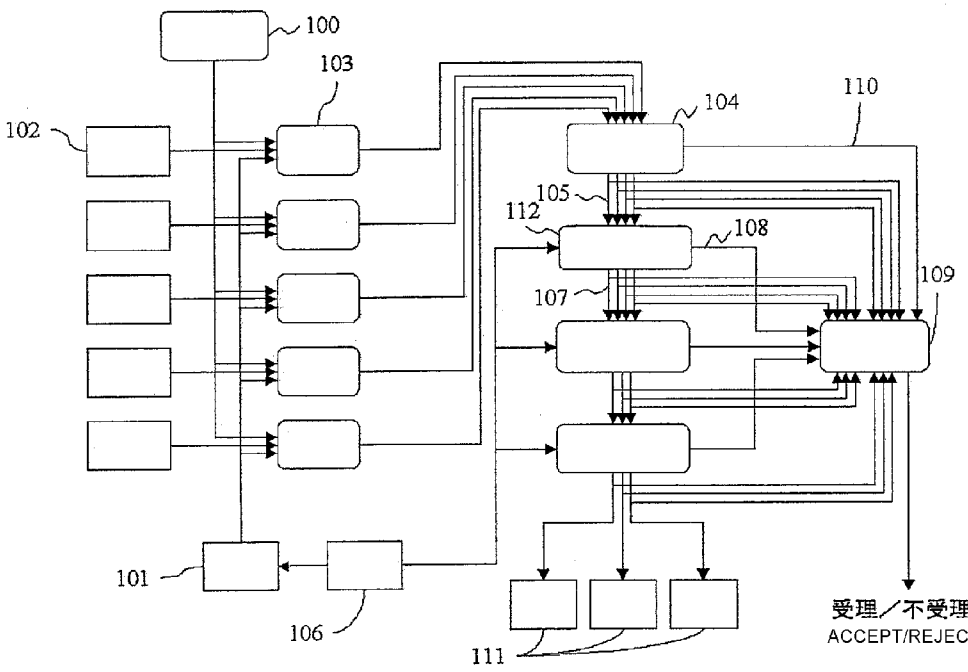
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM,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

[続葉有]

(54) Title: MIXNET SYSTEM

(54) 発明の名称: ミックスネットシステム



(57) Abstract: Each of participant devices (103) uses a common key of common key cryptography to encrypt plaintext, then uses a public key to encrypt the cryptographic key, and then sends them to a respective substituting/decrypting device (112). This can eliminate the limitation of the lengths of encrypted texts to be dealt with. Additionally, a verifying device (109) uses the public key to verify each of certificates issued by the respective substituting/decrypting devices. In this way, even if any one of a plurality of agencies that decrypt and substitute encrypted texts has not performed correct operations, a third party can determine such an agency and certify that the determined agency is an unauthorized one.

[続葉有]

WO 2005/071881 A1

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, 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
— 補正書

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。

(57) 要約: 各参加者装置103が、平文を共通鍵暗号方式の共通鍵を使用して暗号化すると共に、上記暗号鍵を公開鍵により暗号化し、これらを置換復号装置112へ送付する。これにより、扱うことのできる暗号文の長さに制限をなくすことができる。また、本発明では、各置換復号装置が行った、公開鍵を利用した検証可能な証明文を、検証装置109が公開鍵を利用して検証する。これにより、暗号文の復号と入れ替えを行う複数の機関の中に操作を正しく行わなかったものが存在した場合、これを第三者が特定し、特定されたものが不正者であることを証明できる。