

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2008 年 1 月 31 日 (31.01.2008)

PCT

(10) 国際公開番号
WO 2008/013212 A1

(51) 国際特許分類:

H04L 9/14 (2006.01) G06K 19/073 (2006.01)
G06K 17/00 (2006.01) H04L 9/08 (2006.01)
G06K 19/07 (2006.01)

(TERUYAMA, Katsuyuki) [JP/JP]; 〒1080075 東京都
港区港南 1 丁目 7 番 1 号 ソニー株式会社内 Tokyo
(JP).

(21) 国際出願番号: PCT/JP2007/064633

(22) 国際出願日: 2007 年 7 月 26 日 (26.07.2007)

(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2006-203703 2006 年 7 月 26 日 (26.07.2006) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー
株式会社 (SONY CORPORATION) [JP/JP]; 〒1080075
東京都港区港南 1 丁目 7 番 1 号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてののみ): 照山 勝幸

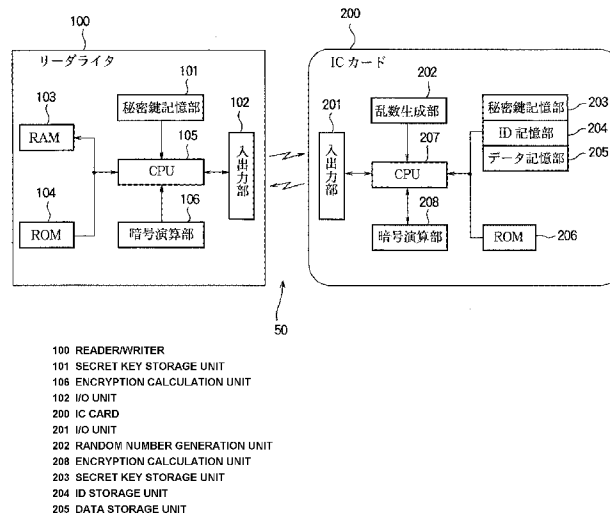
(74) 代理人: 稲本 義雄 (INAMOTO, Yoshio); 〒1600023 東京
都新宿区西新宿 7 丁目 1 1 番 1 8 号 7 1 1 ビル
ディング 4 階 Tokyo (JP).

(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, 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, KE, KG, KM, 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.

[続葉有]

(54) Title: COMMUNICATION SYSTEM AND COMMUNICATION METHOD

(54) 発明の名称: 通信システムおよび通信方法



(57) Abstract: It is possible to provide a communication system and a communication method, an information processing apparatus and method, a device, a program, and recording medium. A reader/writer (100) includes a secret key storage unit (101) containing a plurality of secret keys and identifiers for identifying the secret keys are transmitted to an IC card (200). The IC card (200) reads out a secret key corresponding to the received identifier, encrypts a random number generated by a random number generation unit (202), and transmits it to the reader/writer (100). The reader/writer (100) reads out the secret key stored in the secret key storage unit (101) and corresponding to the identifier transmitted to the IC card (200) in advance and decrypts the encrypted random number received. The present invention can be applied, for example, to an apparatus which performs communication by the NFCIP method.

(57) 要約: 本発明は、簡単な構成で安全且つ利便性の高い情報通信を行うことができる通信システムおよび通信方法、情報処理装置および方法、デバイス、プログラム、並びに記録媒体に関する。リーダライタ 100 の秘密鍵記憶部 101 には、複数の秘密鍵が記憶されており、それらの秘密鍵を特定する識別子が、IC カード 200 に送信される。IC カード 200 は、受信した識別子に対応する秘密鍵を読み出し、乱数生成部 202 に

[続葉有]



WO 2008/013212 A1



(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, MT, 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).

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。

添付公開書類:

— 国際調査報告書

より生成された乱数を暗号化し、リーダライタ100に送信する。リーダライタ100は、秘密鍵記憶部101に記憶され、先にICカード200に送信した識別子に対応する秘密鍵を読み出し、受信した暗号化された乱数を復号する。本発明は、例えば、NFCIP方式で通信を行う装置に適用できる。