

(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
2025年3月13日(13.03.2025)



(10) 国際公開番号

WO 2025/053111 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2024/031502

(22) 国際出願日: 2024年9月2日(02.09.2024)

(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 2023-145654 2023年9月7日(07.09.2023) JP

(71) 出願人: 株式会社 東芝 (KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1050023 東京都港区芝浦一丁目1番1号 Tokyo (JP). 東芝インフラシステムズ株式会社 (TOSHIBA INFRASTRUCTURE SYSTEMS & SOLUTIONS)

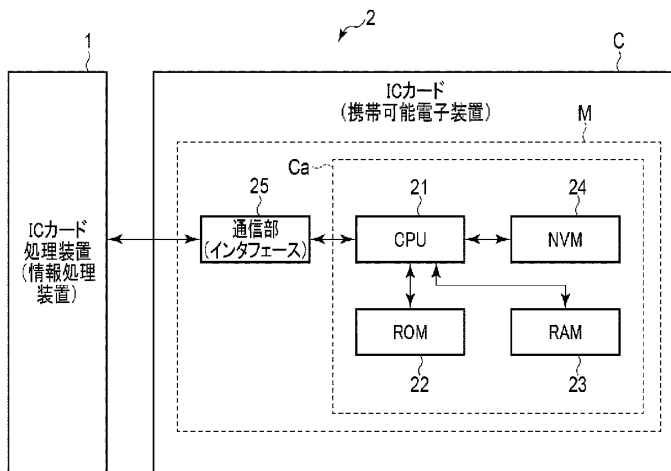
CORPORATION) [JP/JP]; 〒2120013 神奈川県川崎市幸区堀川町7番地34 Kanagawa (JP).

(72) 発明者: 福田 亜紀 (FUKUDA, Aki); 〒2120013 神奈川県川崎市幸区堀川町7番地34 東芝インフラシステムズ株式会社内 Kanagawa (JP). 駒野 雄一 (KOMANO, Yuichi); 〒1050023 東京都港区芝浦一丁目1番1号 株式会社東芝内 Tokyo (JP). 米村 智子 (YONEMURA, Tomoko); 〒1050023 東京都港区芝浦一丁目1番1号 株式会社東芝内 Tokyo (JP).

(74) 代理人: 弁理士法人 鈴榮特許総合事務所 (SUZUYE & SUZUYE); 〒1050014 東京都港区芝三丁目2番1号 セレスティン芝三井ビルディング11階 Tokyo (JP).

(54) Title: PORTABLE ELECTRONIC DEVICE, INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING SYSTEM, AND INFORMATION PROCESSING METHOD

(54) 発明の名称: 携帯可能電子装置、情報処理装置、情報処理システム、及び情報処理方法



- 1 IC card processing device (information processing device)
25 Communication unit (interface)
C IC card (portable electronic device)

(57) Abstract: Provided is a portable electronic device on which a prescribed encryption algorithm can be installed using limited hardware resources. A portable electronic device according to an embodiment comprises a memory, an interface, and a processor. The memory stores encryption information including an encryption algorithm. The interface communicates with an information processing device. The processor generates a random number. The interface transmits the en-

[続葉有]

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, 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).

添付公開書類:

— 国際調査報告 (条約第21条(3))

encryption information to the information processing device, and receives a public key transmitted by the information processing device from among public keys and secret keys generated on the basis of the encryption algorithm. The processor generates an encrypted random number from the random number by means of encryption processing based on the aforementioned public key. The interface transmits the encrypted random number to the information processing device. The processor generates, on the basis of the random number, a session key to be used for communication with the information processing device.

(57) 要約: 限られたハードウェアリソースにて所定の暗号アルゴリズムの搭載を可能とする携帯可能電子装置、を提供すること。実施形態に係る携帯可能電子装置は、メモリ、インタフェース、及びプロセッサを備える。前記メモリは、暗号アルゴリズムを含む暗号情報を記憶する。前記インタフェースは、情報処理装置と通信する。前記プロセッサは、乱数を生成する。また、前記インタフェースは、前記暗号情報を前記情報処理装置へ送信し、前記暗号アルゴリズムに基づき生成される公開鍵及び秘密鍵のうちの前記情報処理装置から送信される前記公開鍵を受信する。前記プロセッサは、前記公開鍵に基づく暗号化処理により前記乱数から暗号化乱数を生成する。前記インタフェースは、前記暗号化乱数を前記情報処理装置へ送信する。前記プロセッサは、前記乱数に基づき前記情報処理装置との通信に使用するセッション鍵を生成する。