

(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
2014年2月13日(13.02.2014)



(10) 国際公開番号

WO 2014/024956 A1

- (51) 国際特許分類:
H04L 9/14 (2006.01) H04L 9/08 (2006.01)
- (21) 国際出願番号: PCT/JP2013/071468
- (22) 国際出願日: 2013年8月8日(08.08.2013)
- (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 2012-175903 2012年8月8日(08.08.2012) JP
特願 2012-176542 2012年8月8日(08.08.2012) JP
- (71) 出願人: 株式会社 東芝 (KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1058001 東京都港区芝浦一丁目1番1号 Tokyo (JP). 東芝ソリューション株式会社 (TOSHIBA SOLUTIONS CORPORATION) [JP/JP]; 〒1056691 東京都港区芝浦一丁目1番1号 Tokyo (JP).
- (72) 発明者: 藤井 吉弘 (FUJII, Yoshihiro); 〒1056691 東京都港区芝浦一丁目1番1号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP). 岡田 光司 (OKADA, Koji); 〒1056691 東京都港区芝浦一丁目1番1号 東芝ソリューション株式会社 技術企画部 知的財産担当内 Tokyo (JP).

Tokyo (JP). 松下 達之 (MATSUSHITA, Tatsuyuki); 〒1058001 東京都港区芝浦一丁目1番1号 株式会社 東芝 知的財産部内 Tokyo (JP). 林 良太郎 (HAYASHI, Ryotaro); 〒1058001 東京都港区芝浦一丁目1番1号 株式会社 東芝 知的財産部内 Tokyo (JP).

(74) 代理人: 蔵田 昌俊, 外 (KURATA, Masatoshi et al.); 〒1050001 東京都港区虎ノ門一丁目三番二号 勤銀不二屋ビル六階 鈴榮特許総合事務所内 Tokyo (JP).

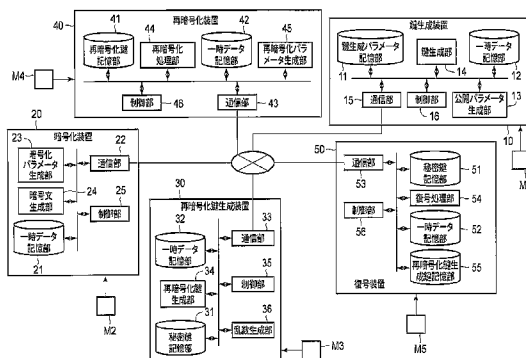
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG,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

[続葉有]

(54) Title: RE-ENCRYPTION KEY GENERATION DEVICE, RE-ENCRYPTION DEVICE, ENCRYPTION DEVICE, DECRYPTION DEVICE, AND PROGRAM

(54) 発明の名称: 再暗号化鍵生成装置、再暗号化装置、暗号化装置、復号装置及びプログラム



- 10 Key generation device
11 Key generation parameter storage unit
12, 21, 32, 42, 52 Temporary data storage unit
13 Public parameter generation unit
14 Key generation unit
15, 22, 33, 43, 53 Communication unit
16, 25, 35, 46, 56 Control unit
20 Encryption device
23 Encryption parameter generation unit
24 Encrypted text generation unit
30 Re-encryption key generation device
31 Private key storage unit
34 Re-encryption key generation unit
36 Random number generation unit
40 Re-encryption device
41 Re-encryption key storage unit
44 Re-encryption processing unit
45 Re-encryption parameter generation unit
50 Decryption device
51 Private key storage unit
54 Decryption processing unit
55 Re-encryption key generation key storage unit

(57) Abstract: This re-encryption key generation device generates a re-encryption key for re-encrypting, without decrypting, encrypted text data obtained by encrypting plaintext data using a first public key of a first user device, and obtaining re-encrypted text data that can be decrypted by a second private key of a second user device. The re-encryption key generation device is provided with a first storage means, a second storage means, and a re-encryption key generation means. The first storage means stores a first private key corresponding to the first public key. The second storage means stores a second re-encryption key generation key of the second user device, which is different from the second public key compatible with the second private key. The re-encryption key generation means generates the re-encryption key on the basis of the first private key and the second re-encryption key generation key.

(57) 要約: 実施形態の再暗号化鍵生成装置は、第1ユーザ装置の第1公開鍵により平文データを暗号化して得られた暗号文データを復号せずに再暗号化して、第2ユーザ装置の第2秘密鍵により復号可能な再暗号文データを得るための再暗号化鍵を生成する。前記再暗号化鍵生成装置は、第1記憶手段、第2記憶手段及び再暗号化鍵生成手段を備えている。前記第1記憶手段は、前記第1公開鍵に対応する第1秘密鍵を記憶する。第2記憶手段は、前記第2秘密鍵に対応する第2公開鍵とは異なる前記第2ユーザ装置の第2再暗号化鍵生成鍵を記憶する。前記再暗号化鍵生成手段は、前記第1秘密鍵及び前記第2再暗号化鍵生成鍵に基づいて、前記再暗号化鍵を生成する。



MZ, NA, RW, SD, SL, 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, 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))