

(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
2012 年 11 月 1 日(01.11.2012)



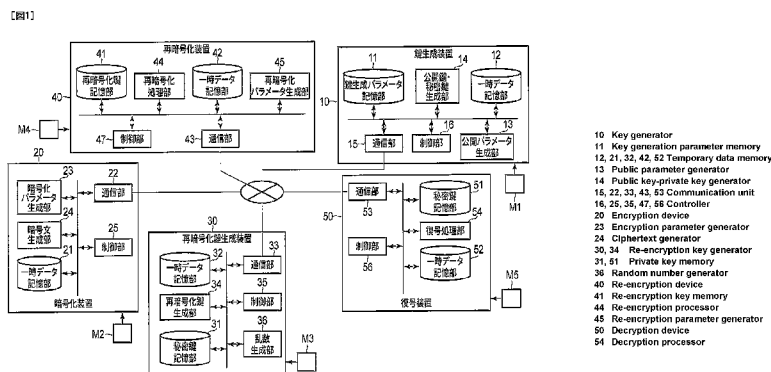
(10) 国際公開番号
WO 2012/147869 A1

- (51) 国際特許分類:
H04L 9/30 (2006.01) H04L 9/14 (2006.01)
- (21) 国際出願番号: PCT/JP2012/061256
- (22) 国際出願日: 2012 年 4 月 26 日(26.04.2012)
- (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 2011-099563 2011 年 4 月 27 日(27.04.2011) JP
- (71) 出願人 (米国を除く全ての指定国について): 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; および
- (75) 発明者/出願人 (米国についてのみ): 林 良太郎 (HAYASHI, Ryotaro) [JP/JP]. 松下 達之 (MAT-SUSHITA, Tatsuyuki) [JP/JP]. 藤井 吉弘 (FUJII, Yoshihiro) [JP/JP]. 吉田 琢也 (YOSHIDA, Takuya) [JP/JP]. 岡田 光司 (OKADA, Koji) [JP/JP].
- (74) 代理人: 蔵田 昌俊, 外 (KURATA, Masatoshi et al.); 〒1050001 東京都港区虎ノ門 1 丁目 1 2 番 9 号 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, 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, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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, ML, MR, NE, SN, TD, TG).

[続葉有]

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

(54) 発明の名称: 再暗号化鍵生成装置、再暗号化装置及びプログラム



(57) Abstract: A re-encryption key generator according to an embodiment re-encrypts, without decrypting, ciphertext data obtained by encrypting plaintext data by means of a first public key of a first user device, and generates a re-encryption key for obtaining re-encrypted text data capable of being decrypted by means of a second private key of a second user device. The re-encryption key generator is provided with a first memory means, a second memory means, a first random number generation means, and a re-encryption key generation means. The first memory means stores a first private key corresponding to the first public key. The second memory means stores a second public key corresponding to the second private key. The first random number generation means generates a first random number. The re-encryption key generation means generates the re-encryption key based on the first private key, the second public key, and the first random number.

(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、第 1 乱数生成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 公開鍵を記憶する。前記第 1 乱数生成手段は、第 1 乱数を生成する。前記再暗号化鍵生成手段は、前記第 1 秘密鍵、前記第 2 公開鍵及び前記第 1 乱数に基づいて、前記再暗号化鍵を生成する。

WO 2012/147869 A1



添付公開書類:

— 国際調査報告 (条約第 21 条(3))