(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
2013 年 4 月 4 日(04.04.2013)

WIPO | PCT

(10) 国際公開番号
WO 2013/047291 A1

(51) 国際特許分類:
H04L 9/14 (2006.01) *H04L 9/08* (2006.01)
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2012/073914

(22) 国際出願日: 2012 年 9 月 19 日(19.09.2012)

(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 2011-217616 2011 年 9 月 30 日(30.09.2011) 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: 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). 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). 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). 吉田 琢也 (YOSHIDA, Takuya); 〒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).

(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１２番９号 鈴榮特許綜合事務所内 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, 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, PA, 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.

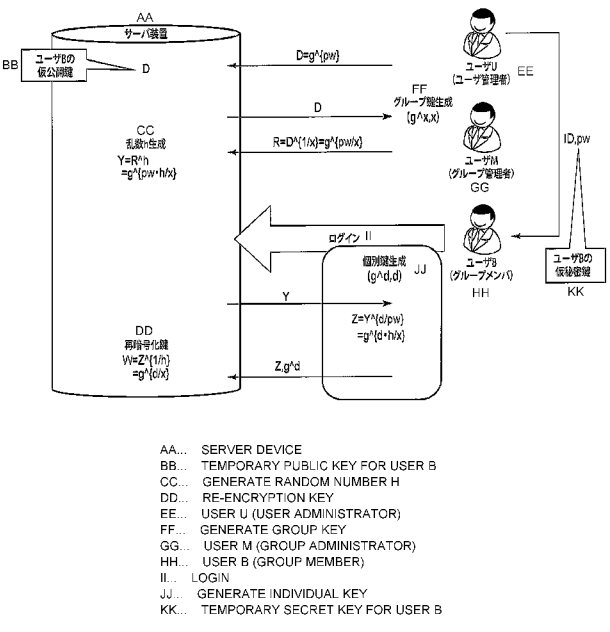
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW,

[続葉有]

(54) **Title**: SERVER DEVICE AND PROGRAM

(54) 発明の名称 : サーバ装置及びプログラム

[図4]



AA... SERVER DEVICE
BB... TEMPORARY PUBLIC KEY FOR USER B
CC... GENERATE RANDOM NUMBER H
DD... RE-ENCRYPTION KEY
EE... USER U (USER ADMINISTRATOR)
FF... GENERATE GROUP KEY
GG... USER M (GROUP ADMINISTRATOR)
HH... USER B (GROUP MEMBER)
II... LOGIN
JJ... GENERATE INDIVIDUAL KEY
KK... TEMPORARY SECRET KEY FOR USER B

(57) **Abstract**: A server device of the embodiment, upon receiving a notification from a user device that a re-encryption key is to be updated, generates a random number in order to calculate re-encryption key information on the basis of a stored re-encrytion key and the generated random number. The server device transmits the re-encryption key information to the user device in order to receive, from the user device, re-encryption key update information calculated from the re-encryption key information on the basis of the user secret key before the update and a user secret key after the update. The server device calculates a re-encrytion key after the update on the basis of the re-encryption key update information and the random number, and replaces the re-encryption key within storage means with the re-encryption key after the update.

(57) 要約: 実施形態のサーバ装置は、ユーザ装置から再暗号化鍵を更新する旨の通知を受けると、乱数を生成し、記憶された再暗号化鍵及び前記生成した乱数に基づいて再暗号化鍵情報を計算する。前記サーバ装置は、前記再暗号化鍵情報を前記ユーザ装置に送信し、前記ユーザ装置から更新前の前記ユーザ秘密鍵及び更新後のユーザ秘密鍵に基づいて当該再暗号化鍵情報から計算された再暗号化鍵更新情報を受信する。前記サーバ装置は、前記再暗号化鍵更新情報及び前記乱数に基づいて前記更新後の再暗号化鍵を計算すると共に、前記記憶手段内の再暗号化鍵を前記更新後の再暗号化鍵に置換する。

WO 2013/047291 A1

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).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）