

(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10月3日(03.10.2013)



(10) 国際公開番号

WO 2013/145796 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01) H04L 9/32 (2006.01)
G09C 1/00 (2006.01)
- (21) 国際出願番号: PCT/JP2013/050226
- (22) 国際出願日: 2013年1月9日(09.01.2013)
- (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 2012-074773 2012年3月28日(28.03.2012) 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). 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).

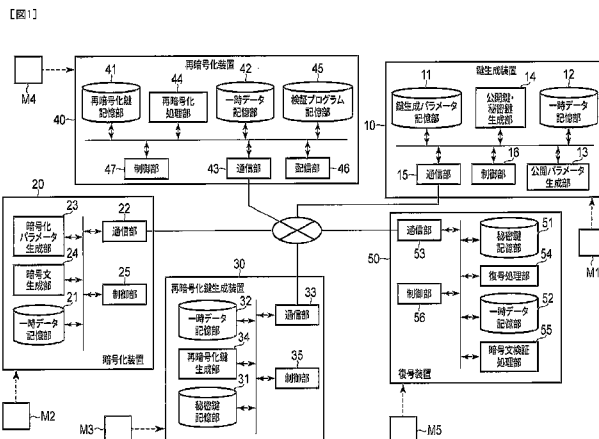
(74) 代理人: 蔵田 昌俊, 外 (KURATA, Masatoshi et al.); 〒1050001 東京都港区虎ノ門1丁目12番9号 鈴榮特許総合事務所内 Tokyo (JP).

(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, 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,

[続葉有]

(54) Title: RE-ENCRYPTED TEXT VERIFICATION PROGRAM, RE-ENCRYPTION DEVICE, AND RE-ENCRYPTION SYSTEM

(54) 発明の名称: 再暗号文検証プログラム、再暗号化装置及び再暗号化システム



- 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... PUBLIC KEY/PRIVATE KEY GENERATION UNIT
15, 22, 33, 43, 53... COMMUNICATION UNIT
16, 25, 35, 45, 55... CONTROL UNIT
20... ENCRYPTION DEVICE
23... ENCRYPTION PARAMETER GENERATION UNIT
24... ENCRYPTED TEXT GENERATION UNIT
30... RE-ENCRYPTION KEY GENERATION DEVICE
31, 51... PRIVATE KEY STORAGE UNIT
34... RE-ENCRYPTION KEY GENERATION UNIT
40... RE-ENCRYPTION DEVICE
41... RE-ENCRYPTION KEY STORAGE UNIT
44... RE-ENCRYPTION PROCESSING UNIT
45... VERIFICATION PROGRAM STORAGE UNIT
46... DELIVERY UNIT
50... DECRYPTION DEVICE
54... DECRYPTION PROCESSING UNIT
55... ENCRYPTED TEXT VERIFICATION PROCESSING UNIT

(57) Abstract: In a decryption device of an embodiment according to the present invention, a retaining means pre-retain a portion of re-encrypted text data used in a re-encryption system, as well as a verification formula that holds true if a public key, which is used in encryption processing for encrypted text data prior to re-encryption processing of the re-encrypted text data, and a private key making it possible to decode the re-encrypted text data are plugged in. A determining means plugs the portion of re-encrypted text data received from the re-encryption device, the public key of a re-encryption key generation device fetched from a fourth storing means, and the private key of the decryption device into the verification formula, and performs calculation on the basis of the verification formula fetched from the storing means, and thereby determines whether or not the verification formula holds true. An outputting means outputs a verification success when the result of this determination is that the verification formula holds true.

(57) 要約:

[続葉有]



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).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

実施形態の復号装置において、保持手段は、前記再暗号化システムに用いられる再暗号文データの一部と、当該再暗号文データを再暗号化処理する前の暗号文データの暗号化処理に用いられた公開鍵と、当該再暗号文データを復号可能な秘密鍵とが代入された場合に成立する検証式を予め保持する。判定手段は、前記保持手段から読み出した検証式に基づき、前記再暗号化装置から受けた再暗号文データの一部と、前記第 4 記憶手段から読み出した前記再暗号化鍵生成装置の公開鍵と前記復号装置の秘密鍵とを当該検証式に代入して演算を実行することにより、この検証式が成立するか否かを判定する。出力手段は、この判定の結果、前記検証式が成立したとき、検証成功を出力する。