(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
2006 年9 月8 日 (08.09.2006)

PCT

(10) 国際公開番号
WO 2006/092909 A1

(51) 国際特許分類:
H04L 9/32 (2006.01)

(21) 国際出願番号: PCT/JP2006/300068

(22) 国際出願日: 2006 年1 月6 日 (06.01.2006)

(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2005-054087 2005 年2 月28 日 (28.02.2005) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目７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): 古川 潤 (FURUKAWA, Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: 宮崎 昭夫, 外(MIYAZAKI, Teruo et al.); 〒1070052 東京都港区赤坂１丁目９番２０号 第１６興和ビル８階 Tokyo (JP).

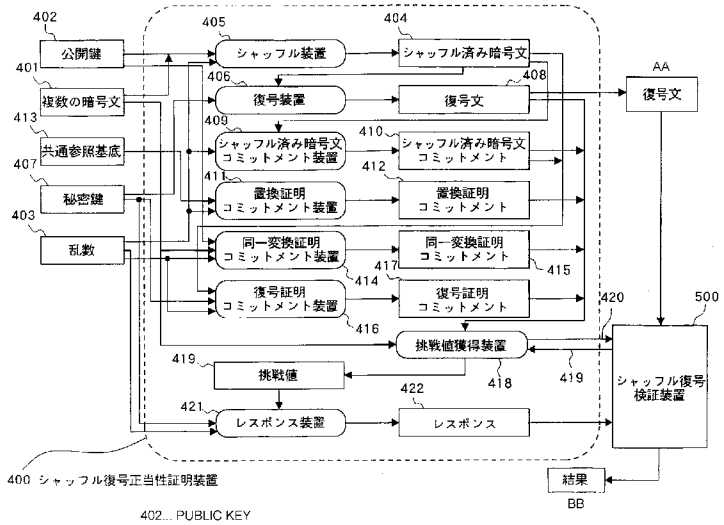
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO,

[続葉有]

WO 2006/092909 A1

(54) Title: SHUFFLE DECRYPTION VALIDITY VERIFYING DEVICE AND METHOD, SHUFFLE DECRYPTION VALIDATING DEVICE AND METHOD, PROGRAM AND RECORDING MEDIUM

(54) 発明の名称: シャッフル復号正当性証明装置と方法、シャッフル復号検証装置と方法、プログラムと記録媒体



402... PUBLIC KEY
401... ENCRYPTED TEXTS
413... COMMON REFERENCE BASE
407... SECRET KEY
403... RANDOM NUMBER
405... SHUFFLE DEVICE
406... DECRYPTING DEVICE
409... SHUFFLED ENCRYPTED TEXT COMMITMENT DEVICE
411... REPLACEMENT VERIFICATION COMMITMENT DEVICE
414... SAME CONVERSION VERIFICATION COMMITMENT DEVICE
416... DECRYPTION VERIFICATION COMMITMENT DEVICE
419... CHALLENGE VALUE
421... RESPONSE DEVICE
404... SHUFFLED ENCRYPTED TEXT
408... DECRYPTED TEXT
410... SHUFFLED ENCRYPTED TEXT COMMITMENT
412... REPLACEMENT VERIFICATION COMMITMENT
415... SAME CONVERSION VERIFICATION COMMITMENT
417... DECRYPTION VERIFICATION COMMITMENT
418... CHALLENGE VALUE ACQUIRING DEVICE
422... RESPONSE
AA..... DECRYPTED TEXT
500... SHUFFLE DECRYPTION VALIDATING DEVICE
BB..... RESULT
400... SHUFFLE DECRYPTION VALIDITY VERIFYING DEVICE

(57) Abstract: A shuffle decryption verification for verifying the validity of shuffle and decryption with higher security without leaking knowledge of all secret information. In a shuffle decryption validity verifying device, encryption texts, a public key, a decrypting secret key, and a random number are inputted, the encryption texts are encrypted, their order is rearranged, decrypted texts are created by decrypting the encrypted texts by means of the secret key, and the validity of the encryption, order rearrangement, and decryption for a shuffle decryption validating device is verified. The commitment of the shuffled encrypted texts which are the encrypted texts created by encrypting the encryption texts with the public key and rearranging their order is included in the data communicated with the shuffle decryption validating device.

(57) 要約: 本発明は、シャッフルと復号の正当性を証明するにあたり、一切の秘密情報に関する知識を漏らさないことで、より強い安全性を持ったシャッフル復号証明を行なうことを目的とするもので、複数の暗号文と、公開鍵と、復号の秘密鍵と、乱数と、が入力され、複数の暗号文を公開鍵によりそれぞれ暗号化し、それらの順番を入れ替え、秘密鍵によりそれぞれ復号した結果である複数の復号文を生成し、暗号化と順番の入れ替えと復号とに対する正当性をシャッフル復号検証装置に対して証明するシャッフル復号正当性証明装置において、シャッフル復号検証装置と通信するデー

[続葉有]

RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

タに、複数の暗号文を公開鍵により暗号化し、その順番を入れ替えた暗号文であるシャッフル済み暗号文のコミットメントを含める。