(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
2008 年6 月19 日 (19.06.2008)

PCT

(10) 国際公開番号
WO 2008/072455 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2007/072551

(22) 国際出願日: 2007 年11 月21 日 (21.11.2007)

(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 2006-333882
2006 年12 月11 日 (11.12.2006) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1080075 東京都港区港南１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): 白井 太三 (SHIRAI, Taizo) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 渋谷 香士 (SHIBUTANI, Kyoji) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 秋下 徹 (AKISHITA, Toru) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 盛合 志帆 (MORIAI, Shiho) [JP/JP]; 〒1070062 東京都港区南青山２丁目６番２１号 株式会社ソニー・コンピュータエンタテインメント内 Tokyo (JP).

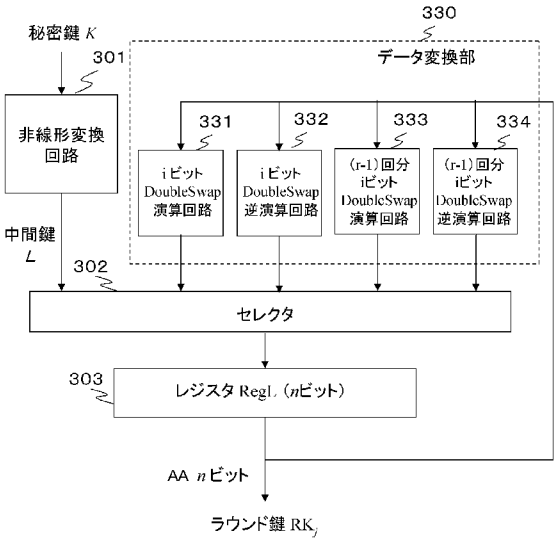
(74) 代理人: 宮田 正昭, 外(MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目１番７号 銀座ティーケイビル 澤田・宮田・山田・佐々木特許事務所 Tokyo (JP).

(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, BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK,

/続葉有/

(54) **Title:** ENCRYPTION DEVICE, ENCRYPTION METHOD, AND COMPUTER PROGRAM

(54) **発明の名称:** 暗号処理装置、および暗号処理方法、並びにコンピュータ・プログラム



K SECRET KEY
301 NONLINEAR CONVERSION CIRCUIT
L INTERMEDIATE KEY
330 DATA CONVERSION UNIT
331 i-BIT Double Swap OPERATION CIRCUIT
332 i-BIT Double Swap INVERSE OPERATION CIRCUIT
333 (r-1)-TIME i-BIT Double Swap OPERATION CIRCUIT
334 (r-1)-TIME i-BIT Double Swap INVERSE OPERATION CIRCUIT
302 SELECTOR
303 REGISTER RegL (*n* BITS)
AA *n* BITS
RK_j ROUND KEY

(57) **Abstract:** It is possible to realize a common key block encryption configuration capable of increasing key analysis difficulty and safety. An intermediate key generated by conversion of a secret key is stored in a register and a round key is generated by conversion of data stored in the register. The round key is generated by swap of partial data constituting the data stored in the register. For example, the data in the register is divided into four partial data so as to obtain two sets of partial data having identical number of bits. Each of the partial data is subjected to swap repeatedly so as to generate a plurality of different round keys. With this configuration, the bit arrangement of each round key is effectively exchanged and it is possible to generate round keys having a low correlation and realize a highly safe encryption which increases the key analysis difficulty.

(57) **要約:** 鍵解析の困難性を高め、安全性を高めた共通鍵ブロック暗号処理構成を実現する。秘密鍵の変換処理によって生成した中間鍵をレジスタに格納して、レジスタ格納データの変換処理によりラウンド鍵を生成する構成において、レジスタ格納データを構成する部分データのスワップ（入れ替え）処理を実行してラウンド鍵を生成する。例えば、等しいビット数を持つ部分データの組を２組設定するように４つの部分データに区分し、各部分データのスワップ処理を繰り返し実行して、複数の異なるラウンド鍵を生成する。本構成により、各ラウンド鍵のビット配列が効果的に入れ替わり相関性の低いラウンド鍵の生成が可能となり、鍵の解析困難性を高めた安全性の高い暗号処理が実現される。

WO 2008/072455 A1

SL, SM, SV, SY, 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, 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, MT, 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