

(43) 國際公開日  
2012 年 10 月 4 日(04.10.2012)



(10) 国際公開番号

WO 2012/132620 A1

- (51) 国際特許分類:  
H04L 9/06 (2006.01) G09C 1/00 (2006.01)
- (21) 国際出願番号: PCT/JP2012/053930
- (22) 国際出願日: 2012 年 2 月 20 日(20.02.2012)
- (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 2011-069182 2011 年 3 月 28 日(28.03.2011) JP  
特願 2011-207702 2011 年 9 月 22 日(22.09.2011) 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): 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

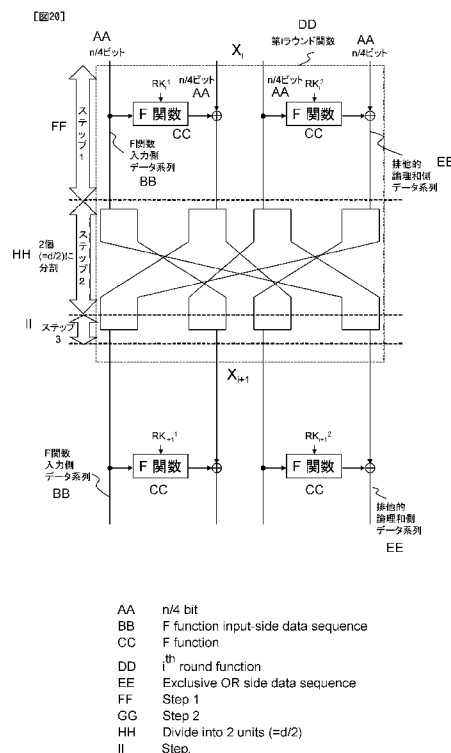
社内 Tokyo (JP). 五十部 孝典 (ISOBE, Takanori) [JP/JP]; 〒1080075 東京都港区港南1丁目7番1号 ソニー株式会社内 Tokyo (JP). 白井 太三 (SHIRAI, Taizo) [JP/JP]; 〒1080075 東京都港区港南1丁目7番1号 ソニー株式会社内 Tokyo (JP). 樋渡 玄良 (HIWATARI, Harunaga) [JP/JP]; 〒1080075 東京都港区港南1丁目7番1号 ソニー株式会社内 Tokyo (JP). 三津田 敦司 (MITSUDA, Atsushi) [JP/JP]; 〒1080075 東京都港区港南1丁目7番1号 ソニー株式会社内 Tokyo (JP).

- (74) 代理人: 宮田 正昭, 外(MIYATA, Masaaki et al.);  
〒1040032 東京都中央区八丁堀三丁目25番9  
号 KSKビル西館8階 特許業務法人 大同  
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, 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, 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,

[続葉有]

- (54) Title: ENCRYPTION PROCESSING DEVICE, ENCRYPTION PROCESSING METHOD, AND PROGRAMME  
(54) 発明の名称 : 暗号処理装置、および暗号処理方法、並びにプログラム



**(57) Abstract:** In order to achieve extremely safe encryption processing having improved diffusion properties, one aspect of this invention comprises an encryption processing unit which divides configuration bits of data which is to undergo data processing into a plurality of lines and then inputs the same, and then repeatedly executes a data conversion process, in which a round function is applied, to the data of each line. In the encryption processing unit,  $n/d$  bit data is inputted to each line, said  $n/d$  bit data being  $n$  bit data, which is input data, divided by a division number ( $d$ ), and an operation including a data conversion process to which a round function is applied is repeatedly executed as a round operation. The  $n/d$  bit data of a line having the output data of the round function is divided by  $d/2$  units, the divided data is combined,  $d$  units of  $n/d$  bit data is reconfigured, said data differing from the output data of the round operation of the previous stage, and a process making the input data for the round operation of the next stage is executed. Due to this configuration, extremely safe encryption processing having improved diffusion properties can be achieved.

(57) 性的の構一のデリ入dしし／合n力

上させた安全性の高い暗号処理が実現される。



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, MD, 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))