

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2002 年 10 月 17 日 (17.10.2002)

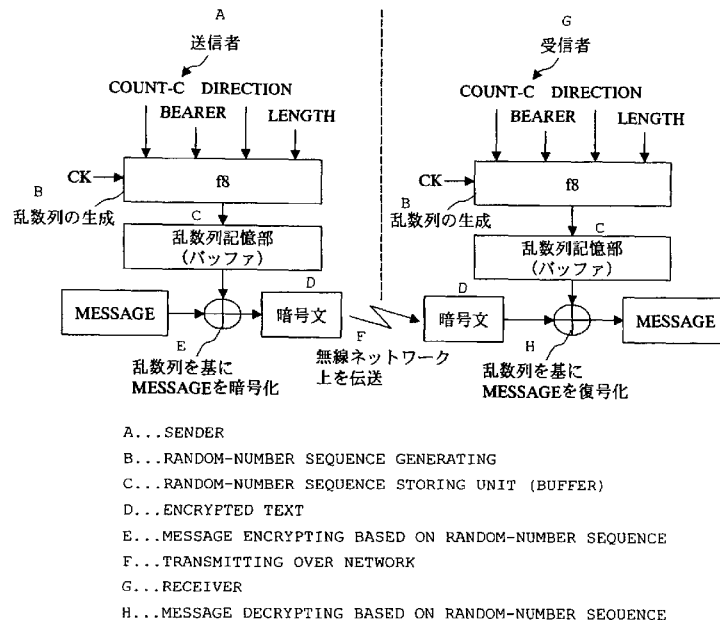
PCT

(10) 国際公開番号
WO 02/082715 A1

- (51) 国際特許分類⁷: H04L 9/00, G09C 1/00 [JP/JP]. 宇賀晋介 (UGA, Shinsuke) [JP/JP]: 〒100-8310 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP01/02880
- (22) 国際出願日: 2001 年 4 月 3 日 (03.04.2001) (74) 代理人: 溝井章司, 外(MIZOI, Shoji et al.); 〒247-0056 神奈川県鎌倉市大船二丁目17番10号 NTA大船ビル 3F Kanagawa (JP).
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語 (81) 指定国 (国内): AU, CA, CN, JP, KR, MX, NO, SG, US.
- (71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 Tokyo (JP). (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 粕谷智巳 (KASUYA, Tomomi) [JP/JP]. 近澤 武 (CHIKAZAWA, Takeshi) [JP/JP]. 若林隆夫 (WAKABAYASHI, Takao)
- 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。

(54) Title: ENCRYPTING DEVICE

(54) 発明の名称: 暗号化装置



(57) Abstract: A random-number sequence is generated in advance by a data concealing function f8 that generates a random-number sequence and is stored in a random-number sequence storing unit (buffer). When data (message) is input, a random-number sequence stored in the random-number sequence storing unit is retrieved and the data (message) is encrypted in an EXCLUSIVE-OR circuit to prepare an encrypted text. When decoding data, a random-number sequence is generated by the data concealing function f8 for storing in the random-number sequence storing unit (buffer). When an encrypted text is input, a random-number sequence is read from the random-number sequence storing unit (buffer) in the EXCLUSIVE-OR circuit for decrypting to data (message).

[続葉有]



WO 02/082715 A1



(57) 要約:

乱数列を生成するデータ秘匿用関数 f_8 により、予め乱数列を生成し、乱数列記憶部（バッファ）に記憶しておく。データ（メッセージ）が入力された場合に乱数列記憶部に記憶した乱数列を取り出し、排他的論理和演算回路において、データ（メッセージ）を暗号化し、暗号文を作成する。データを復号する場合にも、データ秘匿用関数 f_8 において、予め乱数列を発生し、乱数列記憶部（バッファ）に記憶しておく。暗号文が入力された場合に、排他的論理和演算回路において、乱数列記憶部（バッファ）から乱数列を読み出し、データ（メッセージ）に復号化する。