

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2006 年 1 月 5 日 (05.01.2006)

PCT

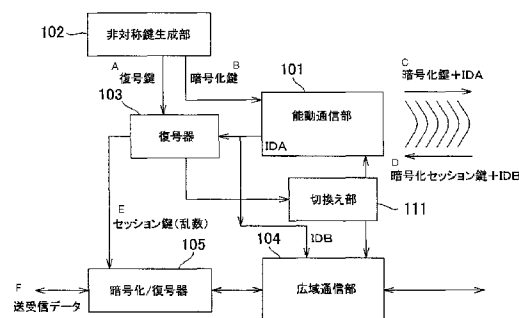
(10) 国際公開番号
WO 2006/001420 A1

- (51) 国際特許分類⁷: H04L 9/08, 12/28 (74) 代理人: 中村 友之 (NAKAMURA, Tomoyuki); 〒1050001 東京都港区虎ノ門 1 丁目 2 番 8 号 虎ノ門琴平タワー 三好内外国特許事務所内 Tokyo (JP).
- (21) 国際出願番号: PCT/JP2005/011735
- (22) 国際出願日: 2005 年 6 月 27 日 (27.06.2005)
- (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2004-190192 2004 年 6 月 28 日 (28.06.2004) 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]; 〒1410001 東京都品川区北品川 6 丁目 7 番 3 5 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): 高山 佳久 (TAKAYAMA, Yoshihisa). 森田 直 (MORITA, Tadashi).
- (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, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, 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,

[続葉有]

(54) Title: COMMUNICATION SYSTEM AND COMMUNICATION DEVICE

(54) 発明の名称: 通信システム及び通信装置



20

102... ASYMMETRIC KEY GENERATION UNIT
A... ENCRYPTION KEY
B... DECRYPTION KEY
103... DECRYPTER
101... ACTIVE COMMUNICATION UNIT
C... ENCRYPTION KEY + IDA
D... ENCRYPTED SESSION KEY + IDB
111... SWITCHING UNIT
E... SESSION KEY (RANDOM NUMBER)
F... TRANSMISSION/RECEPTION DATA
105... ENCRYPTER/DECRYPTER
104... WIDE-RANGE COMMUNICATION UNIT

(57) Abstract: There is provided a communication device capable of easily identifying a communication partner even when the communication device does not have a high processing ability and securely sharing a session key with the communication partner. The communication device includes a proximity active communication unit (101) for transmitting an enquiry signal via an electromagnetic wave to an approaching external communication device and waiting for a response to the enquiry signal; a wide-range communication unit (104) capable of performing communication via an electromagnetic wave in a range larger than the communication-enabled range of the proximity active communication means; a switching unit (111) for switching to one of the communication units: a proximity active communication unit and a wide-range communication unit; an asymmetric key generation unit (102) for generating a pair of an encryption key and a decryption key corresponding to the encryption key. The communication device uses the decryption key to decrypt the encrypted session key transmitted by the external communication device and transmits a communication switching request signal requesting the external communication device to switch to the wide-range communication unit for communication.

(57) 要約: 通信装置の処理能力が高くなくとも通信相手を容易に特定し、双方でセキュアにセッション鍵を共有することが可能な通信装置を提供する。近接する外部通信装置に対し電磁波を介して問合せ信号を送信し、該問合せ信号の応答を待ち受ける近接能動通信部 101 と; 近接能動通信手段の通信可能領域よりも広い範囲で電磁波を介して通信可能な広域通信部 104 と; 近接能動通信部または広域通信部のうちいずれか一方の通信部に切替える切換

[続葉有]

WO 2006/001420 A1



BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,
IE, IS, IT, LT, LU, 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).

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。

添付公開書類:

— 国際調査報告書

え部111と；一組の暗号化鍵と該暗号化鍵に対応する復号鍵とを生成する非対称鍵生成部102とを備えており、復号鍵を用いて、外部通信装置によって送信される暗号化されたセッション鍵を復号するとともに、外部通信装置に対し、広域通信部に切換えて通信することを要求する通信切換え要求信号を送信することを特徴とする、通信装置が提供される。