9705601-4
IPOS

06 JUL 1999

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6: H04L 9/08, H04K 1/00, H04B 17/00 — A1

(11) International Publication Number: WO 96/22643

(43) International Publication Date: 25 July 1996 (25.07.96)

(21) International Application Number: PCT/US96/00785

(22) International Filing Date: 19 January 1996 (19.01.96)

(30) Priority Data:
(1) 08/376,144 — 20 January 1995 (20.01.95) — US

(71) Applicant: ERICSSON, INC. [US/US]; One Triangle Drive, P.O. Box 13969, Research Triangle Park, NC 27709 (US).

(72) Inventors: HASSAN, Amer, A.; P.O. Box 12485, Durham, NC 27709 (US). HERSHEY, John, E.; 4 Vines Road, Ballston Lake, NY 12019 (US). CHENNAKESHU, Sandeep; 204-H Hyde Park Court, Cary, NC 27513 (US).

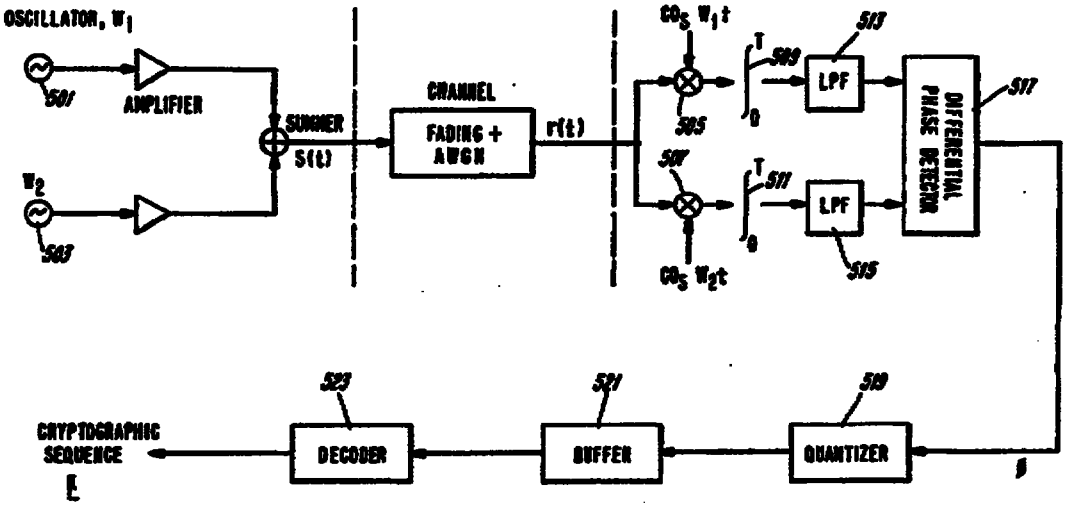
(74) Agents: GRUDZIECKI, Ronald, L. et al.; Burns, Doane, Swecker & Mathis, L.L.P., P.O. Box 1404, Alexandria, VA 22313-1404 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AZ, BY, KG, KZ, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

1 PD
1 applⁿ.
3 invs.

(54) Title: ESTABLISHMENT OF CRYPTOGRAPHIC KEYS IN RADIO NETWORKS



(57) Abstract

Characteristics of the radio channel are used to establish key sequences for use in encrypting communicated information. These characteristics are the short-term reciprocity and rapid spatial decorrelation of phase of the radio channel. The keys can be established with computations equivalent to a bounded distance decoding procedure, and the decoder used to establish a key may be used for processing the subsequent data transmission. Compared to classical and public-key systems, an alternative mechanism for establishing and sharing key sequences that depends on a physical process is provided in which each party need not generate a pseudorandom quantity because the necessary randomness is provided by the temporal and spatial non-stationarity of the communication channel itself. By using a channel decoder, the probability of two users establishing the same secret key is substantially unity, and the probability of an eavesdropper establishing the same key is substantially zero. Also, the number of possible keys is large enough that finding the correct one by exhaustive search is impractical.