PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/08 — A1

(11) International Publication Number: WO 97/49213

(43) International Publication Date: 24 December 1997 (24.12.97)

(21) International Application Number: PCT/US97/09348

(22) International Filing Date: 6 June 1997 (06.06.97)

(30) Priority Data:
08/665,339 17 June 1996 (17.06.96) US

(71) Applicant: ERICSSON INC. [US/US]; 7001 Development Drive, P.O. Box 13969, Research Triangle Park, NC 27709 (US).

(72) Inventors: HASSAN, Amer, A.; 412 Key West Mews, Cary, NC 27513 (US). HERSHEY, John, E.; 4 Vines Road, Ballston, NY 12019 (US). CHENNAKESHU, Sandeep; 311 Glen Abbey Drive, 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).

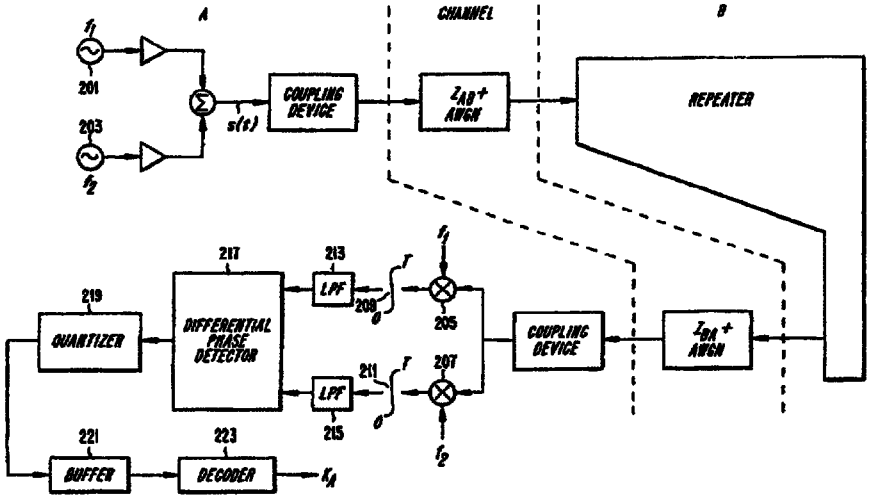
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, 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.

(54) Title: APPARATUS AND METHOD FOR SECURE COMMMUNICATION BASED ON CHANNEL CHARACTERISTICS



(57) Abstract

Characteristics of a communication channel are used to establish key sequences for use in encrypting communicated information. In one embodiment, these characteristics are the impedances of the channel viewed from one transceiver to the other and vice versa. 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 cryptographic 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 pseudo-random quantity because the necessary randomness is provided by the properties 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.