



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : H04L 9/08		A1	(11) International Publication Number: WO 00/65768
			(43) International Publication Date: 2 November 2000 (02.11.00)
(21) International Application Number: PCT/EP00/03284		(81) Designated States: AE, AG, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), DM, DZ, EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 11 April 2000 (11.04.00)			
(30) Priority Data: 60/130,944 26 April 1999 (26.04.99) US 09/461,766 15 December 1999 (15.12.99) US			
(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (publ) [SE/SE]; S-126 25 Stockholm (SE).			
(72) Inventors: PERSSON, Joakim; Iliongränden 147, S-224 72 Lund (SE). SMEETS, Ben; Dalbackavägen 11, S-240 10 Dalby (SE). HANSSON, Mattias; Kämnärsvägen 13 C:101, S-226 46 Lund (SE).			
(74) Agent: ERICSSON MOBILE COMMUNICATIONS AB; IPR Department, S-221 83 Lund (SE).		Published <i>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.</i>	

(54) Title: METHOD AND DEVICE FOR EFFECTIVE KEY LENGTH CONTROL

(57) Abstract

The present invention includes a method and device for calculating an encryption key, K'_c , for use in the initialization of an encryption algorithm. The present invention discloses a method for calculating the encryption key, $K'_c(x)$, by obtaining a ciphering key, $K_c(x)$, determining a maximum ciphering key length, L , based on the requirements of the two devices wishing to communicate, and determining a maximum usable encryption key length, L_{max} . The ciphering key, $K_c(x)$, is then manipulated through an addition function or an exclusively-or function with a polynomial $g_1(x)$. The result is multiplied with a polynomial $g_2(x)$, which spreads the starting points of said encryption key, $K'_c(x)$. The encryption key is thus determined according to $K'_c(x) = g_2^{(L)}(x)[K_c(x) \bmod g_1^{(L)}(x)]$. The method of calculating the encryption key, K'_c , ensures that a maximum ciphering key length is not exceeded. In addition, the method provides new possible starting points each time a new encryption key, K'_c , is generated.

