



(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/04* (2009.01)

(21) International Application Number:
PCT/FI2010/050509

(22) International Filing Date:
16 June 2010 (16.06.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/494,957 30 June 2009 (30.06.2009) US

(71) Applicant (for all designated States except US): **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FI-02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **KUBOTA, Keiichi** [JP/GB]; 71 A Thames Street, Weybridge Surrey KT13 8LP (GB).

(74) Agent: **NOKIA CORPORATION**; IPR Department, Virpi Tognetty, Keilalahdentie 4, FI-02150 Espoo (FI).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: SYSTEMS, METHODS, AND APPARATUSES FOR CIPHERING ERROR DETECTION AND RECOVERY

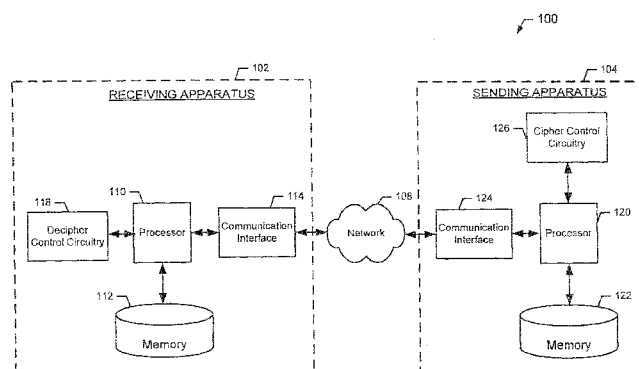


FIG. 1.

(57) Abstract: Systems, methods, and apparatuses are provided for ciphering error detection and recovery. A method may include using a first set of one or more cipher input parameters to decipher ciphered data ciphered using a second set of one or more cipher input parameters. The method may further include comparing a value of at least a portion of the deciphered data to an expected value. The method may additionally include determining an occurrence of a ciphering error when the value of the at least a portion of the deciphered data is not equal to the expected value. The method may also include initiating a ciphering resynchronization procedure in response to the determination that a ciphering error occurred so as to resynchronize at least one of the first set of cipher input parameters with at least one of the second set of cipher input parameters. Corresponding systems and apparatuses are also provided.