(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 March 2006 (30.03.2006)

PCT

(10) International Publication Number
WO 2006/033013 A3

(51) International Patent Classification:
H04L 9/06 (2006.01)

(21) International Application Number:
PCT/IB2005/003104

(22) International Filing Date:
20 September 2005 (20.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

2004905507	24 September 2004 (24.09.2004)	AU
2004906543	16 November 2004 (16.11.2004)	AU
2004907361	30 December 2004 (30.12.2004)	AU
2004907374	31 December 2004 (31.12.2004)	AU
2005902136	29 April 2005 (29.04.2005)	AU

(71) Applicant *(for all designated States except US)*: **SYNAPTIC LABORATORIES LIMITED** [CH/CH]; 6 rue Verdaine, PO Box 3122, CH-1211 Geneva 1 (CH).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **O'NEIL, Sean** [AU/AU]; 255/421 Brunswick St, Fortitude Valley QLD 4006 (AU).

(74) Agent: **EVANS, Allen, John**; 5/238 The Avenue, Parkville, Victoria 3052 (AU).

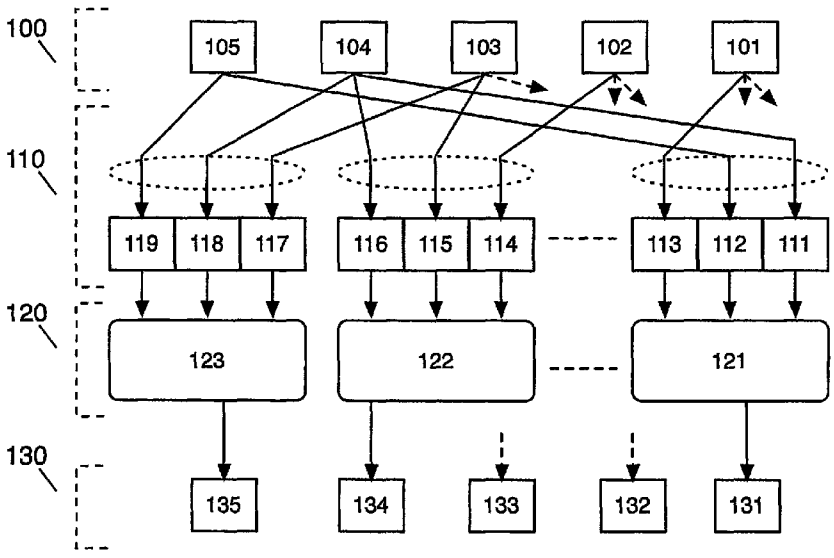
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, 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) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, 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).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SUBSTITUTION BOXES



(57) Abstract: A multiple-input multiple-output s-box receives *a* contiguously numbered input bits (101, 102, 103, 104, *105)*I_1, I_2 to I_a, where *a* is at least 4, and outputs *b* contiguously numbered output bits (131, 132, 133, 134, 135) O_1, O_2, to O_b. The s-box comprises *c* primitive s-boxes (121, 122, 123) sb_1 sb_2 to sb_c. Each primitive s-box (121, 122, 123) has a multiple-input single-output Boolean function f_1, f_2, to f_o defining the relationship between the multiple inputs and the single output. Each primitive s-box (121, 122, 123) receives a set of input bitss_1, s_2, to s_c, respectively, each such set is chosen from the *a* input bits (101, 102, 103, 104, 105) to the s-box and containing sl_1, sl_2, to sl_c bits respectively. Each of the numbers sl_1, sl_2, to sl_c is in the range of 3 to (*a*-1), and the sum of the numbers sl_1, sl_2, to sl_c is larger than *a*. The *b* output bits of the s-box (131, 132, 133, 134, 135) are the outputs of the c Boolean functions.

WO 2006/033013 A3

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
15 June 2006

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.