



(51) International Patent Classification:  
**H04L 9/16** (2006.01)

(21) International Application Number:  
PCT/AU2010/001222

(22) International Filing Date:  
20 September 2010 (20.09.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
61/246,531 29 September 2009 (29.09.2009) US

(71) Applicant (for all designated States except US): **SILVERBROOK RESEARCH PTY LTD** [AU/AU]; 393 Darling Street, Balmain, New South Wales 2041 (AU).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **STARR, Matthew Raymond** [AU/AU]; 393 Darling Street, Balmain, New South Wales 2041 (AU). **PRICE-WHITE, Stephen Cameron** [AU/AU]; 393 Darling Street, Balmain, New South Wales 2041 (AU).

(74) Agent: **SILVERBROOK RESEARCH PTY LTD**; 393 Darling Street, Balmain, New South Wales 2041 (AU).

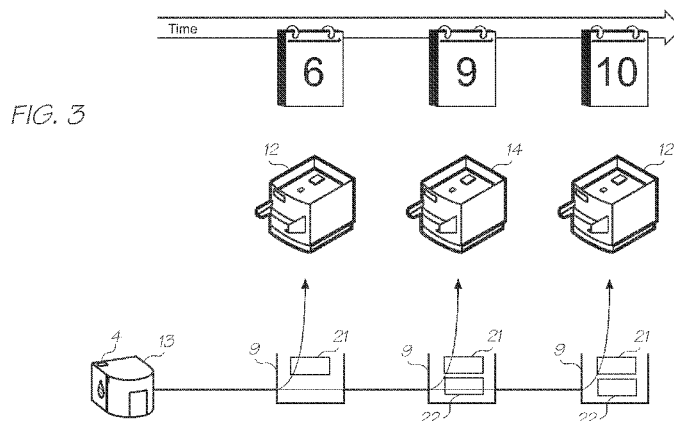
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, 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: COMMUNICATION SYSTEM, METHOD AND DEVICE WITH LIMITED ENCRYPTION KEY RETRIEVAL



(57) Abstract: A method, system and device for encrypted communication with external entities, then device being configured to frustrate side channel attacks attempting to determine an encryption key. The device has a first memory, an encryption key stored in the first memory and a one-way function for application to the encryption key. During use, the encryption key is retrieved from the first memory prior to application to the one-way function and the device is configured to limit the number of times the encryption key is allowed to be retrieved from the non-volatile memory to a pre-determined threshold.