

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
05 October 2017 (05.10.2017)



(10) International Publication Number
WO 2017/173136 A8

(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:

PCT/US2017/025130

(22) International Filing Date:

30 March 2017 (30.03.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/315,415 30 March 2016 (30.03.2016) US

(71) Applicant: **THE ATHENA GROUP, INC.** [US/US]; 408 W. University Avenue, Suite 306, Gainesville, FL 32601 (US).

(72) Inventor: **AUDLEY, Stuart**; c/o The Athena Group, Inc., 408 W. University Avenue, Suite 306, Gainesville, FL 32601 (US).

(74) Agent: **PARKER, James S.** et al.; Saliwanchik, Lloyd & Eisenschenk, PO Box 142950, Gainesville, FL 32614-2950 (US).

(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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

(54) Title: KEY UPDATE FOR MASKED KEYS

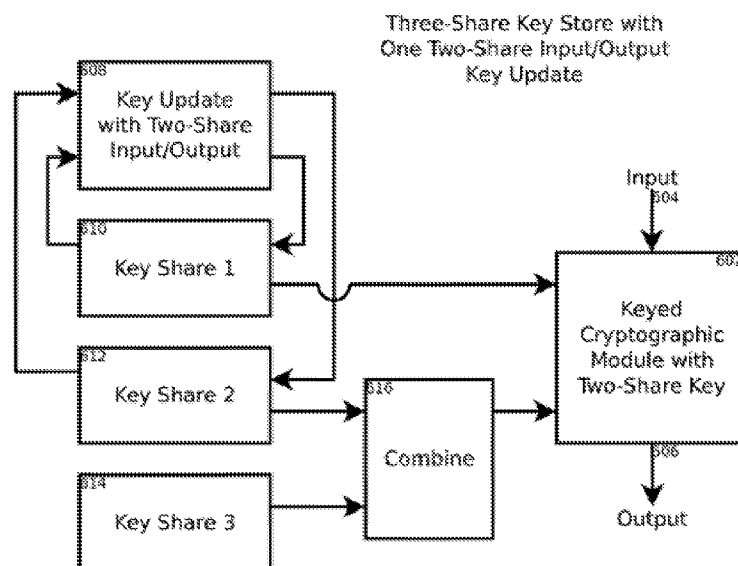


FIG. 6

(57) **Abstract:** Embodiments of the present invention provide methods to perform key updates on key shares of a masked key, which allows updating the masked key without unmasking the masked key (e.g., producing the effective key). By using key shares of a masked key and performing the key update on one or more of the key shares without unmasking the effective key, the cumulative leakage of individual effective keys across multiple cryptographic operations is reduced, and preferably minimized.



EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

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

(48) Date of publication of this corrected version:

09 November 2017 (09.11.2017)

(15) Information about Correction:

see Notice of 09 November 2017 (09.11.2017)