



(51) International Patent Classification:

H04L 29/06 (2006.01)

(21) International Application Number:

PCT/US2014/064738

(22) International Filing Date:

10 November 2014 (10.11.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/902,283 10 November 2013 (10.11.2013) US

14/103,599 11 December 2013 (11.12.2013) US

(71) Applicant: SYPRIS ELECTRONICS, LLC [US/US];
10901 N. McKinley Drive, Tampa, Florida 33612 (US).(72) Inventor: WALLRABENSTEIN, John Ross; 1281 Win
Hentschel Blvd., West Lafayette, Indiana 47906 (US).(74) Agent: BRINDISI, Thomas; 1613 Sunshine Drive, Key
West, Florida 33040 (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, 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, KN, KP, KR,
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, 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).

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a
patent (Rule 4.17(ii))

[Continued on next page]

(54) Title: AUTHENTICATABLE DEVICE

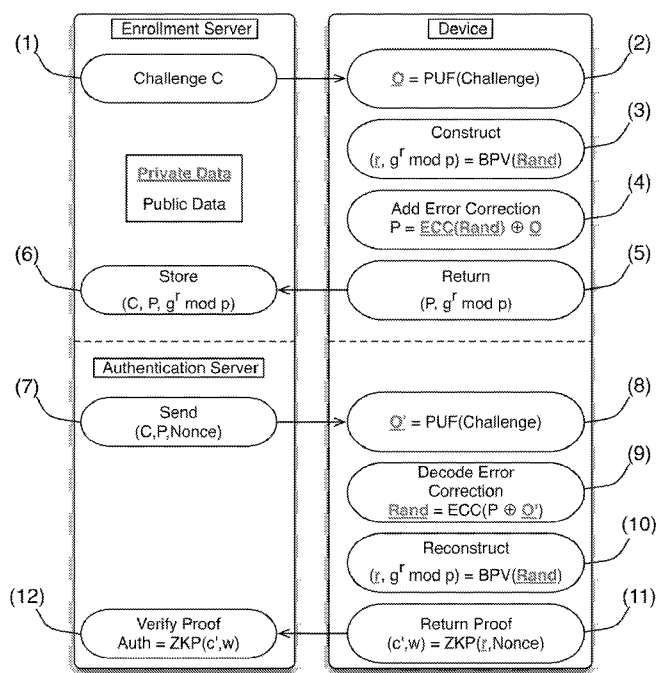


Fig. 1 Enrollment and Authentication Overview

(57) Abstract: An authenticatable device comprising a physically-unclonable function ('PUF') device having a PUF input and a PUF output and constructed to, in response to a challenge C, generate a characteristic output O; a processor, having an input connected to the PUF output, configured to: (1) in response to receipt of output O, generate a commitment value dependent upon a private value r, and (2) in response to contemporaneous receipt of output O and of an authentication query including a nonce, return a zero knowledge proof authentication value that corresponds to the commitment value and to a token that includes a blinded value dependent upon private value r and a random value, the processor being configured to decrypt the random value. An authentication system used with the device preferably has a working verification set including challenge C and commitment value, and a limited verification set including challenge C and a corresponding token.



-
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*
- Published:**
- *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*