

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
11 May 2023 (11.05.2023)



(10) International Publication Number
WO 2023/080842 A3

- (51) International Patent Classification:
H04L 9/32 (2006.01) *G06F 21/64* (2013.01)
- (21) International Application Number:
PCT/SG2022/050769
- (22) International Filing Date:
26 October 2022 (26.10.2022)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
10202112269T 05 November 2021 (05.11.2021) SG
- (71) Applicant: PQCEE PTE LTD [SG/SG]; 7 Temasek Blvd., #12-07 Suntec Tower One, Singapore 038987 (SG).
- (72) Inventors: TAN, Teik Guan; 7 Temasek Blvd., #12-07 Suntec Tower One, Singapore 038987 (SG). ZHOU, Jianying; 8 Somapah Road, Singapore 487372 (SG).
- (74) Agent: SPRUSON & FERGUSON (ASIA) PTE LTD; P.O. Box 1531, Robinson Road Post Office, Singapore 903031 (SG).
- (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,

(54) Title: METHOD AND SYSTEM FOR PROTECTING DIGITAL SIGNATURES

Algorithm 2: Quantum-resistant ECDSA signing $Sign_q$.

```
1 begin
2    $G \leftarrow$  ECC base point;  $P \leftarrow$  ECC order;
3    $\rho \leftarrow$  secret pre-image;
4    $M \leftarrow$  message;
5   Generate signature random  $r$ ;
6   Compute  $r^{-1}$  where  $r * r^{-1} \equiv 1 \text{ mod } P$ ;
7   Compute  $R = (R_x, R_y)$  where  $R \equiv r * G \text{ mod } P$ ;
8   Compute hash of message  $H(M)$ ;
9   Enumerate ZKBoo proof  $\pi =$  begin
10    Zero-knowledge computation of private key  $K_s$  where  $K_s = H(\rho)$ ;
11    Zero-knowledge computation of public key  $K_p$  where
12      $K_p \equiv K_s * G \text{ mod } P$ ;
13    Compute  $s$  where  $s \equiv r^{-1} * (H(M) + R_x * K_s) \text{ mod } P$ ;
14    Commit  $R_x, s$  in the proof;
15  end
16  destroy  $r, r^{-1}, K_s$ ;
17  return  $\sigma = \{R_x, s\}, \pi$ ;
```

200

FIG. 2

(57) Abstract: A method for quantum-resistant digitally signing data, a method for verification of a quantum resistant digital signature for authentication of a source of data by verifying a private key, and a quantum resistant digital signature system are provided. The quantum resistant digital signature system includes a digital signature system and a layer of quantum resistant protection. The digital signature system includes a public key and a private key, wherein the public key is associated with the private key. The digital signature system also includes a digital signature generated in response to data and the private key. The layer of quantum resistant protection is applied to the digital signature system and includes a signing-party-provided quantum-secure proof of knowledge of a pre-image of the private key.

[Continued on next page]

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, ME, 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:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(88) Date of publication of the international search report:

06 July 2023 (06.07.2023)