

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

(19) World Intellectual Property  
Organization  
International Bureau

(43) International Publication Date  
07 April 2022 (07.04.2022)



(10) International Publication Number  
**WO 2022/069132 A1**

(51) International Patent Classification:  
*H04L 9/32* (2006.01)

(21) International Application Number:  
PCT/EP2021/073961

(22) International Filing Date:  
31 August 2021 (31.08.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
2015475.3 30 September 2020 (30.09.2020) GB

(71) Applicant: NCHAIN LICENSING AG [CH/CH]; Grafenauweg 6, 6300 Zug (CH).

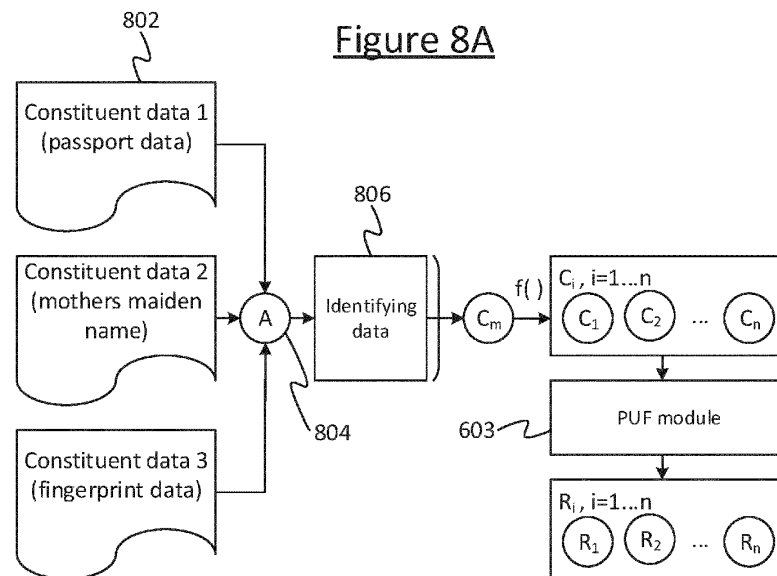
(72) Inventors: DAVIES, Jack, Owen; c/o nChain Licensing AG 30 Market Place, London W1W 8AP (GB). WRIGHT, Craig, Steven; c/o nChain Licensing AG 30 Market Place, London W1W 8AP (GB).

(74) Agent: TOWNSEND, Martyn, James et al.; Bedford House John Street, London WC1N 2BF (GB).

(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, IT, JO, 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, 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, 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,

(54) Title: PHYSICALLY UNCLONABLE FUNCTIONS



(57) Abstract: A method for enabling a verifying party to verify an identity of a target party or device. The method comprises, in a set-up phase: storing, in a data store, a respective piece of response data for each of a set of one or more responses resulting from a setting-up party inputting a respective set of one or more challenges into a PUF module comprising a physically unclonable function, PUF, to generate the one or more responses based on the PUF; and storing an indication of the set of challenges in the data store. The indication does not comprise a value of each of the challenges in the set, but rather a master challenge from which the set of challenges is derivable by applying a derivation function to the master challenge.

[Continued on next page]

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))*