

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
28 April 2022 (28.04.2022)



(10) International Publication Number
WO 2022/086647 A1

(51) International Patent Classification:

G06F 21/32 (2013.01) G06F 21/62 (2013.01)
G06F 21/45 (2013.01) H04L 9/32 (2006.01)
G06F 21/60 (2013.01) H04L 9/30 (2006.01)

(21) International Application Number:

PCT/US2021/050566

(22) International Filing Date:

15 September 2021 (15.09.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

17/079,279 23 October 2020 (23.10.2020) US

(71) Applicant: VISA INTERNATIONAL SERVICE
ASSOCIATION [US/US]; P.O. BOX 8999, SAN
FRANCISCO, California 94128 (US).

(72) Inventors: BADRINARAYANAN, Saikrishna; PO BOX
8999, San Francisco, California 94128 (US). RINDAL, Pe-

ter; PO BOX 8999, San Francisco, California 94128 (US).
MUKHERJEE, Pratay; PO BOX 8999, San Francisco,
California 94128 (US).

(74) Agent: RACZKOWSKI, David B. et al.; Kilpatrick,
Townsend & Stockton LLP, 1100 Peachtree Street Suite
2800, Atlanta, Georgia 30309 (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, 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,

(54) Title: VERIFICATION OF BIOMETRIC TEMPLATES FOR PRIVACY PRESERVING AUTHENTICATION

Parameters: The functionality $\mathcal{F}$ is parameterized by values $\ell, m, \in \mathbb{N}$, $\mathbb{F} \in \mathbb{Z}_{2^m}^\ell$, a distance function $\text{CS.Dist} : \mathbb{Z}_{2^m}^\ell \times \mathbb{Z}_{2^m}^\ell \rightarrow [0, 1]$, a threshold $T \in (0, 1^\ell)$, and leakage functions $L_{\text{dev}}, L_{\text{term}}$ both with description $\mathbb{Z}_m^\ell \times \mathbb{Z}_m^\ell \rightarrow \mathbb{Z}$. It interacts with three parties $\mathcal{D}$, $\mathcal{SP}$ and $\mathcal{T}$ via the following queries.

Queries:

- On receiving a query of the form ("Enrollment", $\text{sid}, \vec{u}, \mathcal{SP}$) from $\mathcal{D}$: Only if sid is unmarked, check if $\|\vec{u}\| = 1$. If the check succeeds, send ("Enrolled", $\text{sid}, \mathcal{D}$) to $\mathcal{SP}$ and $\mathcal{D}$, store $(\text{sid}, \vec{u}, \mathcal{D}, \mathcal{SP})$, and mark sid as "Enrolled". Otherwise, send ("Failed", $\text{sid}, \mathcal{D}$) to $\mathcal{SP}$ and $\mathcal{D}$, and mark sid as "Failed".
- On receiving a query of the form ("Match", $\text{sid}, \text{ssid}, \mathcal{T}$) from $\mathcal{D}$: Check whether sid is marked and there exists a record of the form $(\text{sid}, \vec{u}, \mathcal{D}, \mathcal{SP})$. If the check fails, send ("Failed", $\text{sid}, \text{ssid}, \mathcal{D}$) to $\mathcal{T}$ and $\mathcal{D}$. Else:
 - (1) send $(\text{sid}, \text{ssid}, \mathcal{D})$ to $\mathcal{T}$;
 - (2) receive $(\text{sid}, \text{ssid}, \vec{w}, \mathcal{D})$ from $\mathcal{T}$;
 - (3) if $\langle \vec{u}, \vec{w} \rangle \geq T$, (that is, $\text{CS.Dist}(\vec{u}, \vec{w}) \geq \frac{1}{T^2}$) send $(\text{sid}, \text{ssid}, 1)$ to $\mathcal{D}$ and $\mathcal{T}$, else send $(\text{sid}, \text{ssid}, 0)$. Also send $L_{\text{dev}}(\vec{u}, \vec{w})$ to $\mathcal{D}$ and $L_{\text{term}}(\vec{u}, \vec{w})$ to $\mathcal{T}$.

FIG. 1

(57) **Abstract:** Secure protocols for external-facing authentication are provided for both user templates stored on their devices and the biometric measurement captured by external sensors of an access device. The protocols provide different levels of security, ranging from passive security with some leakage to active security with no leakage. A packing technique is also provided. Zero-knowledge techniques are used during enrollment to validate a norm of user templates and knowledge of the plaintext biometric template. One enrolled, the verifier can sign the encrypted template for use in a later matching phase with an access device.

[Continued on next page]

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 the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

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