

# FIDO UAF

## Registration

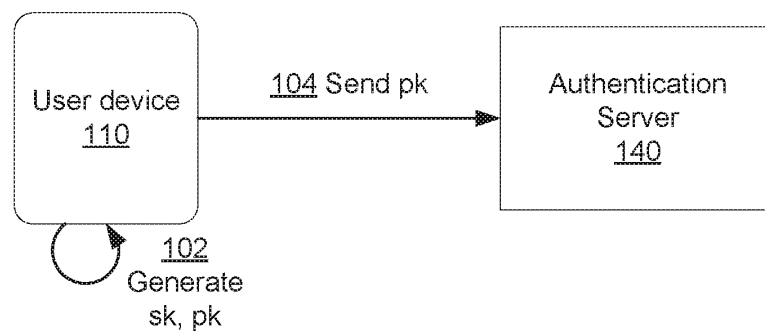


FIG. 1A

## Authentication

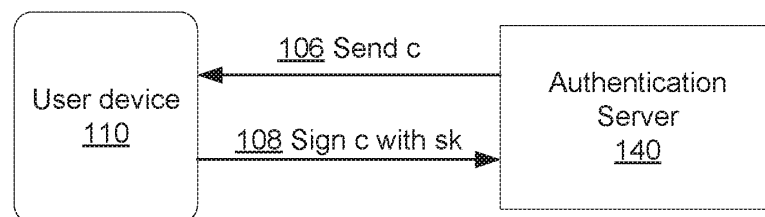


FIG. 1B

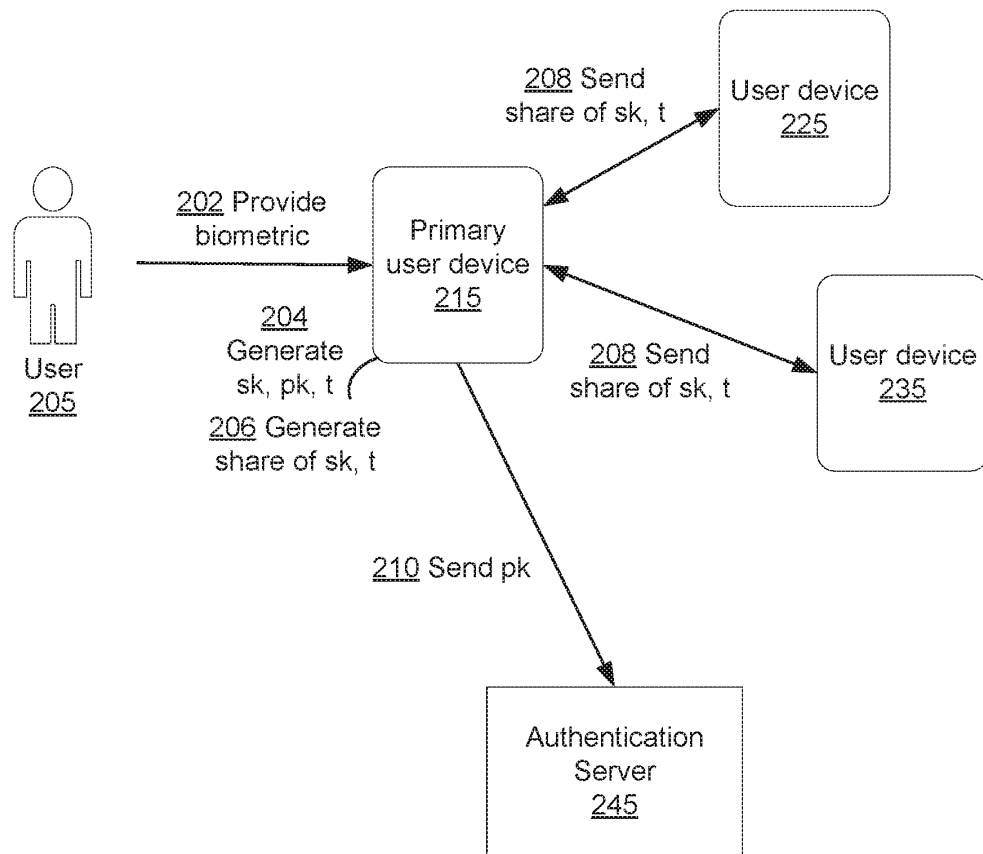


FIG. 2

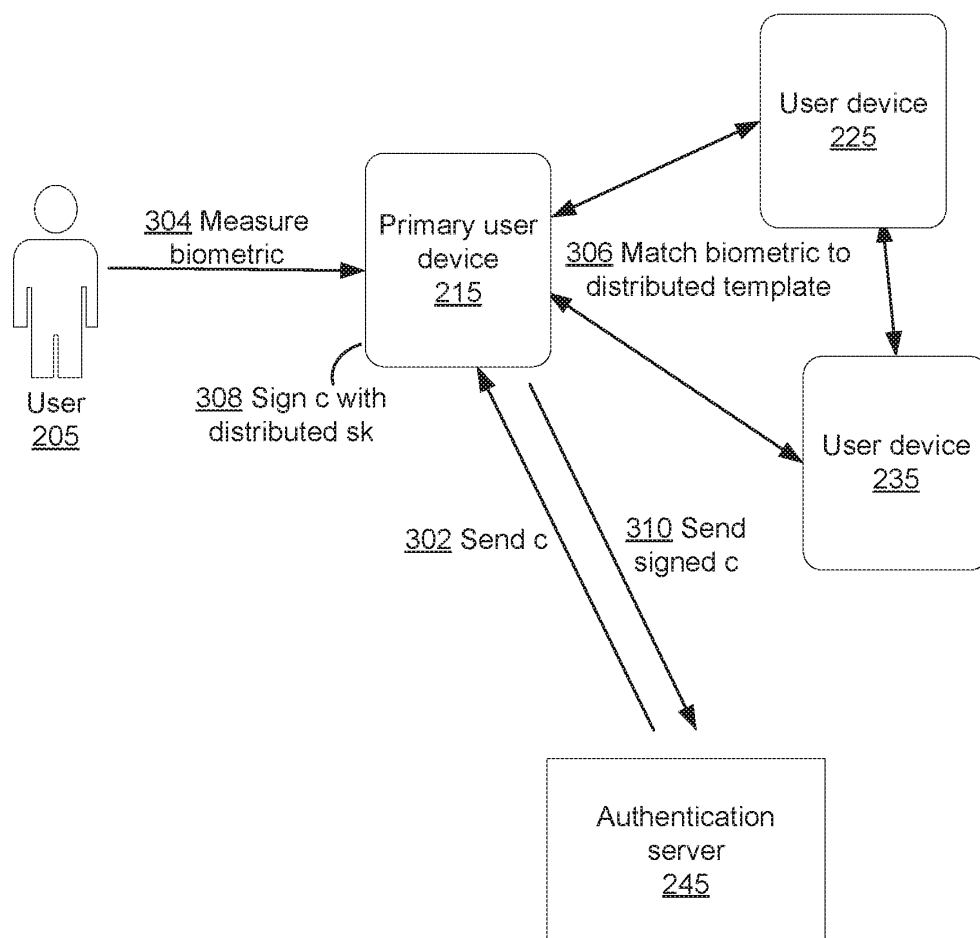


FIG. 3

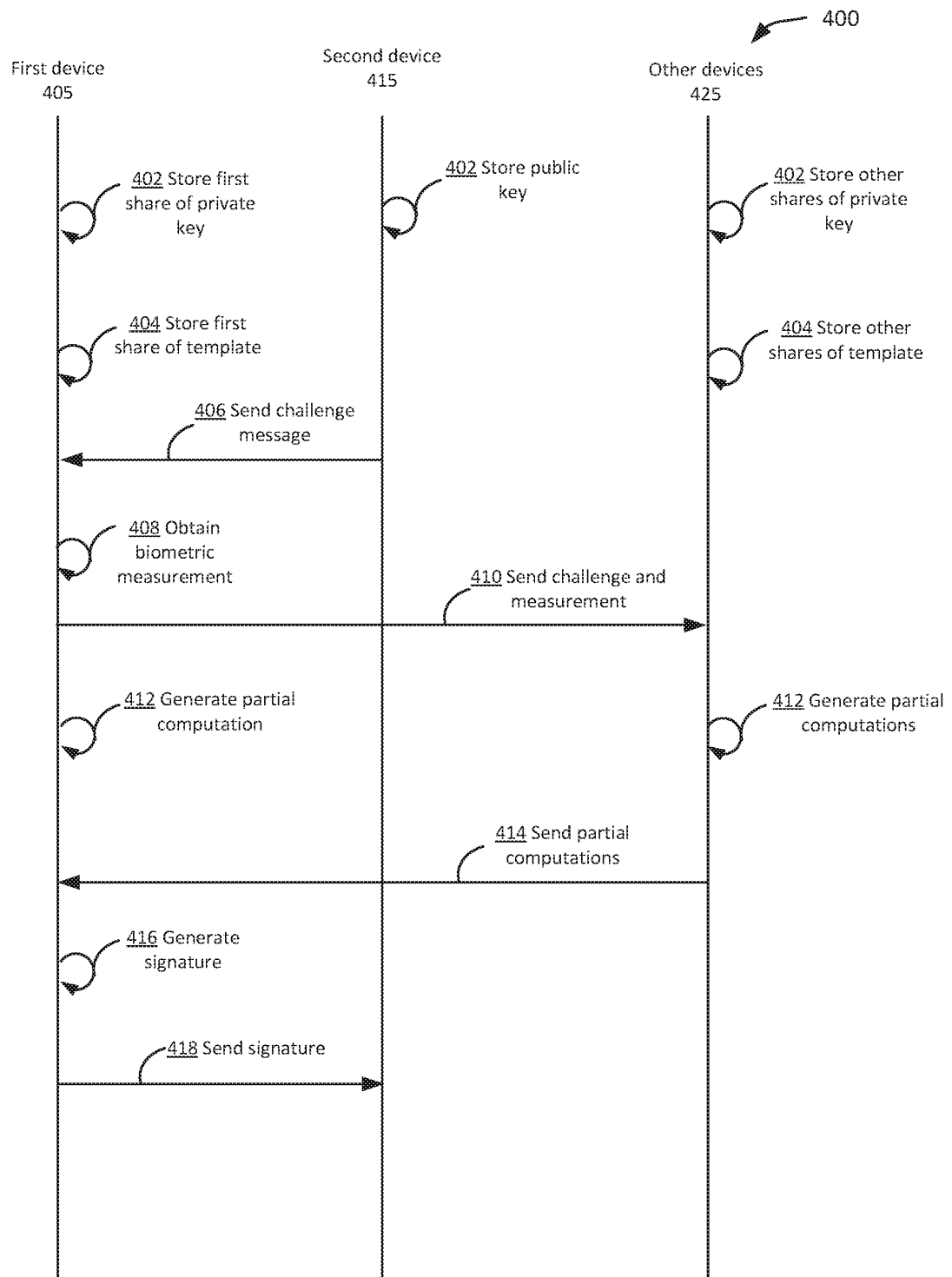


FIG. 4

$\text{Real}_{\mathcal{A}}(1^k, n, t, \text{TS}, q, \ell, d, \mathcal{W}, \tilde{U})$

*Initialization.*

- Run  $([\text{sk}, \tilde{w}]_{[n]}, \text{pp}, \text{vk}) \leftarrow \text{Registration}(1^k, n, t, \text{TS}, q, \ell, \mathcal{W}, d)$  and  $(\text{pp}_{\text{setup}}, s_1, \dots, s_n) \leftarrow \text{Setup}()$ . Give  $(\text{pp}, \text{vk}, \text{pp}_{\text{setup}})$  to  $\mathcal{A}$ .
- $\mathcal{A}$  outputs a corrupt set  $C \subset [n]$  where  $|C| \leq t-1$  and a sequence  $((m_1, j_1, S_1), \dots, (m_h, j_h, S_h))$  where  $S_i \subseteq [n]$ ,  $|S_i| = t$  and  $j_i \in S \setminus C$  for  $i \in [h]$ . Give  $\{(\text{sk}_i, \tilde{w}_i, s_i)\}_{i \in C}$  to  $\mathcal{A}$ . Give  $\text{in}_i := (\text{pp}, \text{sk}_i, \tilde{w}_i, \text{pp}_{\text{setup}}, s_i)$  to party  $i \in [n] \setminus C$ .

*Evaluation.*

- $\mathcal{A}$  can run any number of SignOn sessions with the honest parties.
- $\mathcal{A}$  can also output an integer  $i \in [h]$  indicating that the honest party  $j_i$  initiate a SignOn session with inputs  $(m_i, \tilde{u}_i, S_i)$ .

$\mathcal{F}_{\text{Diffuz}}[1^k, n, t, \text{TS}, q, \ell, d, \mathcal{W}, \tilde{U}]$

*Initialization.*

- Run  $([\text{sk}, \tilde{w}]_{[n]}, \text{pp}, \text{vk}) \leftarrow \text{Registration}(1^k, n, t, \text{TS}, q, \ell, \mathcal{W}, d)$  and give  $(\text{pp}, \text{vk})$  to  $\mathcal{S}$ .
- On message  $(\text{INIT}, (\text{pp}_{\text{setup}}, s_1, \dots, s_n), C, ((m_1, j_1, S_1), \dots, (m_h, j_h, S_h)))$  from  $\mathcal{S}$ , where  $C \subset [n]$ ,  $|C| \leq t-1$ ,  $S_i \subseteq [n]$ ,  $|S_i| = t$  and  $j_i \in S \setminus C$  for  $i \in [h]$ , give  $\{(\text{sk}_i, \tilde{w}_i)\}_{i \in C}$  to  $\mathcal{S}$  and  $\text{in}_i := (\text{pp}, \text{sk}_i, \tilde{w}_i, \text{pp}_{\text{setup}}, s_i)$  to every party  $i \in [n] \setminus C$ .

*Evaluation.*

- On message  $(\text{SIGNON-CORRUPT}, m, \tilde{u}, j, S)$  where  $\tilde{u} \in \mathbb{Z}_q^\ell$ ,  $S \subseteq [n]$ ,  $|S| = t$  and  $j \in S \cap C$ , give  $(m, j, S)$  to every party  $i \in S \setminus C$ . If  $\text{Dist}(\tilde{w}, \tilde{u}) = 1$ , then give  $\text{Sign}(\text{sk}_i, m)$  for all  $i \in S \setminus C$  to  $\mathcal{S}$ .
- On message  $(\text{SIGNON-HONEST}, \text{sid}, i)$  where  $i \in [h]$ , give  $(m_i, j_i, S_i)$  to every party  $i \in S \setminus C$  and store  $(\text{sid}, m_i, \tilde{u}_i, j_i, S_i)$ .
- On message  $(\text{ABORT}, \text{sid})$ , check if there is a tuple of the form  $(\text{sid}, m, \tilde{u}, j, S)$ . If there is, give  $\perp$  to party  $j$ . Delete the tuple.
- On message  $(\text{COMPLETE}, \text{sid})$ , check if there is a tuple of the form  $(\text{sid}, m, \tilde{u}, j, S)$ . If there is, then compute  $\sigma_i := \text{Sign}(\text{sk}_i, m)$  for  $i \in S$  and  $\sigma := \text{Comb}(\{\sigma_i\}_{i \in S})$ . If  $\text{Dist}(\tilde{w}, \tilde{u}) = 1$ , then give  $\sigma$  to party  $j$ . Delete the tuple.

FIG. 5

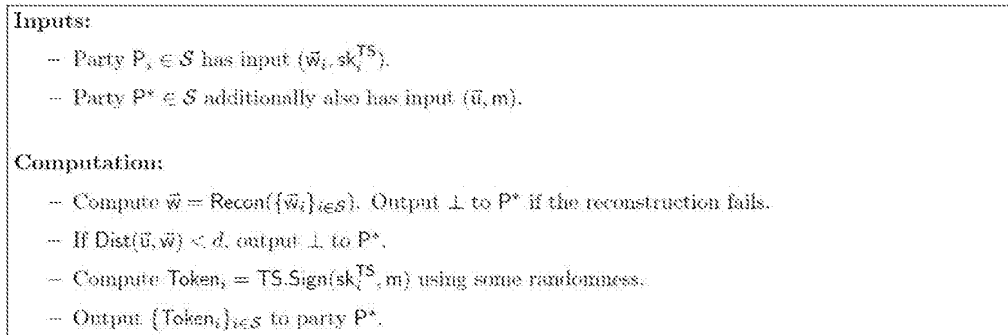


FIG. 6

Hardwired values:  $(a, b, c, d, p, q, r_2, \text{Pad}, d^2)$ .<sup>\*</sup>

Inputs:  $(x_1, x_2, y_1, y_2, z_1, z_2)$ .

Computation:

— Abort if any of the following occur:

- \*  $x_2 \neq (a \cdot x_1 + b)$  (or)
- \*  $y_2 \neq (c \cdot y_1 + d)$  (or)
- \*  $z_2 \neq (p \cdot z_1 + q)$

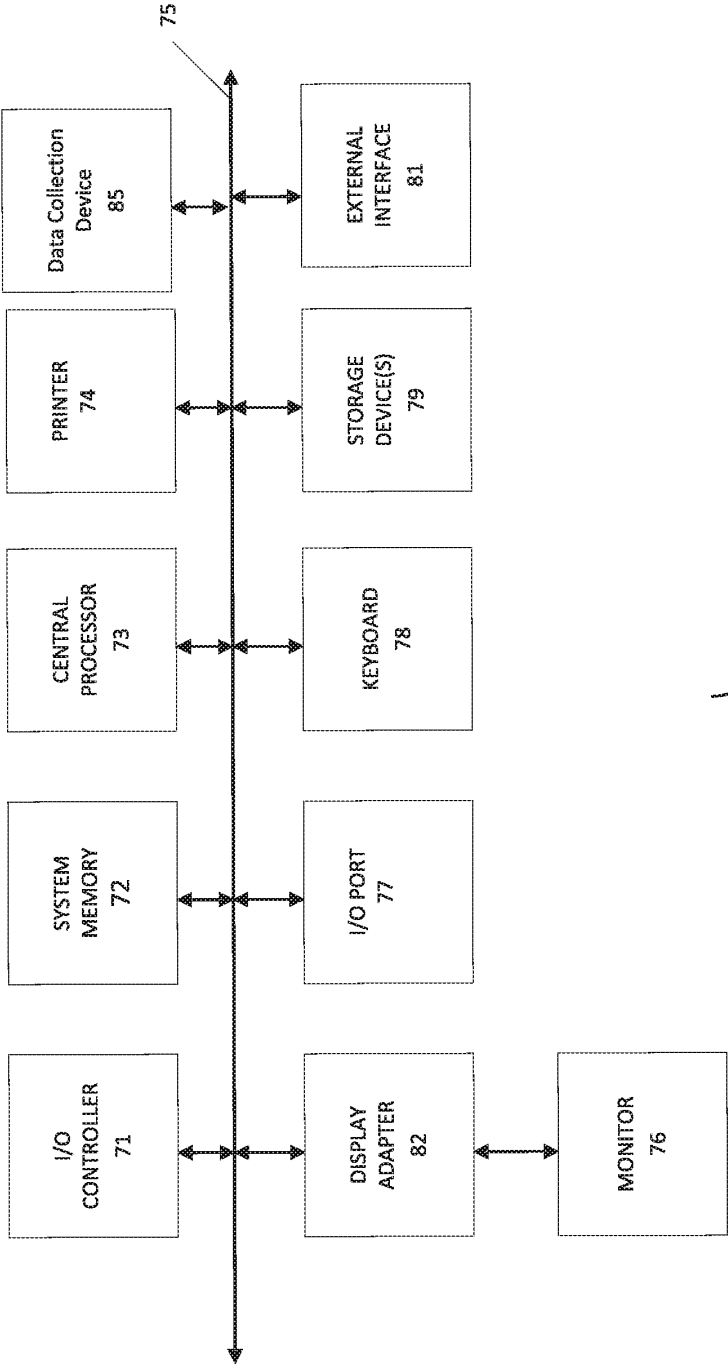
— Compute  $\text{JP} = (z_1 - r_2) + x_1$ .

— If  $\text{JP}^2 > (d^2 \cdot y_1)$ , output Pad. Else, output  $\perp$ .

---

<sup>\*</sup>Recall that  $d$  is the threshold value for Cosine Similarity.

FIG. 7



10

FIG. 8