Sybil-Resistant Identity Systems in Decentralized Environments

BRNO UNIVERSITY OF TECHNOLOGY FACULTY OF INFORMATION TECHNOLOGY

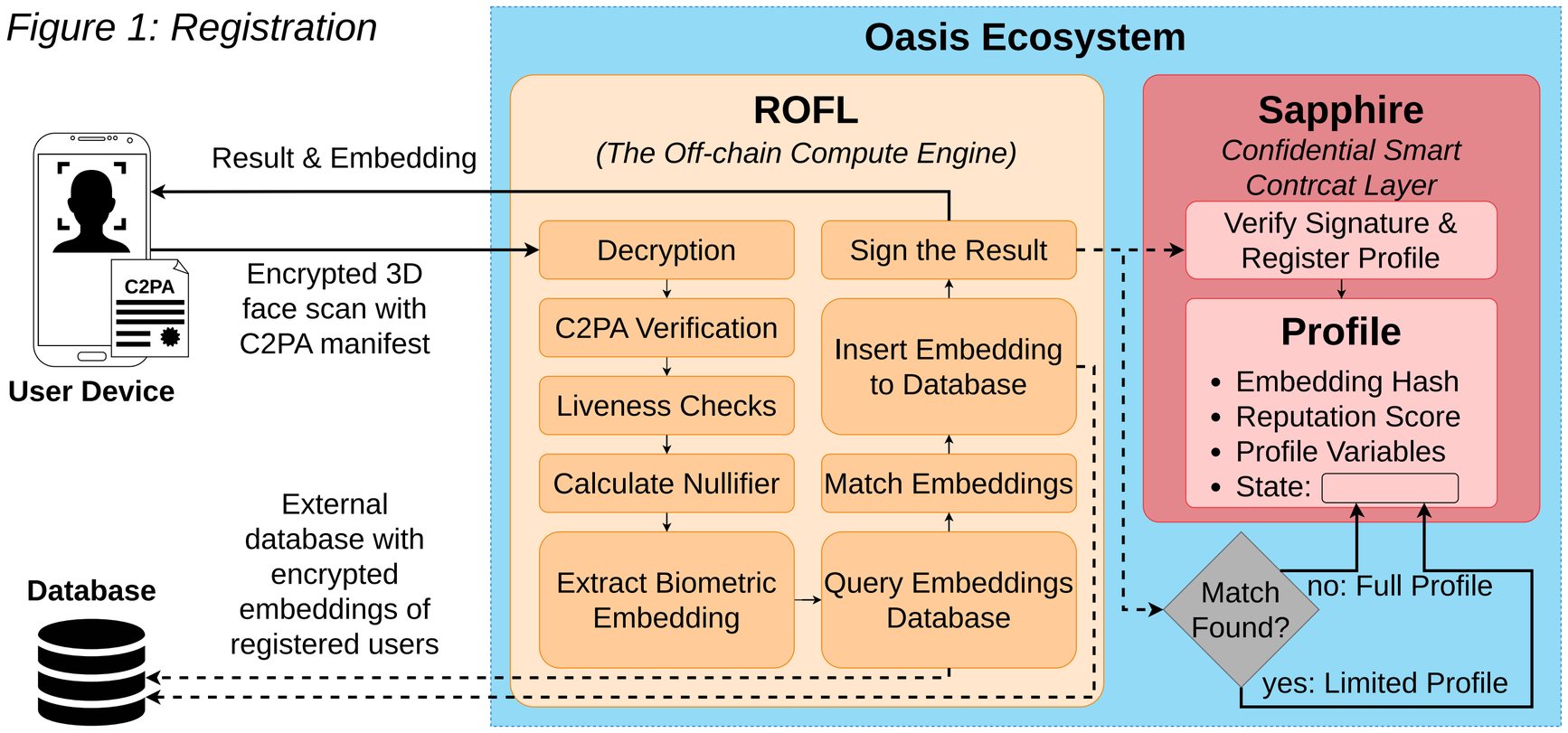
Bc. Michal Ľaš
supervised by doc. Ing. Ivan Homoliak, Ph.D.

Excel@FIT 2026

Goal

Almost all identity management systems, whether centralized or decentralized, use a centralized approach to achieve Sybil resistance – that is, to prevent the creation of a large number of fake identities. Typically, these systems require verification via a phone number or government-issued ID. This project aims to design a decentralized identity system that ensures Sybil resistance while preserving user anonymity and sensitive data. The proposed solution utilizes facial biometric verification and social graph analysis. To ensure decentralization and protect sensitive data privacy, it utilizes blockchain technology, Zero-Knowledge Proofs, and Trusted Execution Environments.

Figure 1: Registration



Registration

User captures a 3D face scan with a C2PA manifest, encrypts it using ROFL's public key, and submits it. Within a TEE, ROFL decrypts the scan to verify the C2PA signature, liveness, and metadata freshness, while ensuring the scan's nullifier is unique.

ROFL then generates a facial embedding, confirms the user is not already registered in the DB, and inserts the new entry.

Finally, the user receives the embedding to store it locally and a signed result to establish their profile on the Sapphire blockchain.

Should facial recognition fail, the user is granted a limited registration and must obtain endorsements from others to complete the process.

Connection Establishment

To establish a connection, two individuals meet in person to exchange identifiers and saved embeddings, while capturing a photo of each other that includes a C2PA manifest and a mutually signed challenge.

Both parties then utilize ROFL for mutual verification, where the system ensures the provided embeddings' hashes are recorded on Sapphire, validates the C2PA manifest and metadata, and matches the photos against the embeddings.

Upon successful verification, ROFL generates a signed connection commitment. At least one user submits this commitment to Sapphire, which verifies the mutual challenge and ROFL signature before checking for existing connections.

Sapphire then blinds the commitment hash with a secret and emits an event for a relayer to add the entry to the Merkle tree. The blinded commitment is also returned to the user if the relayer fails.

Figure 3: Private Random Walks

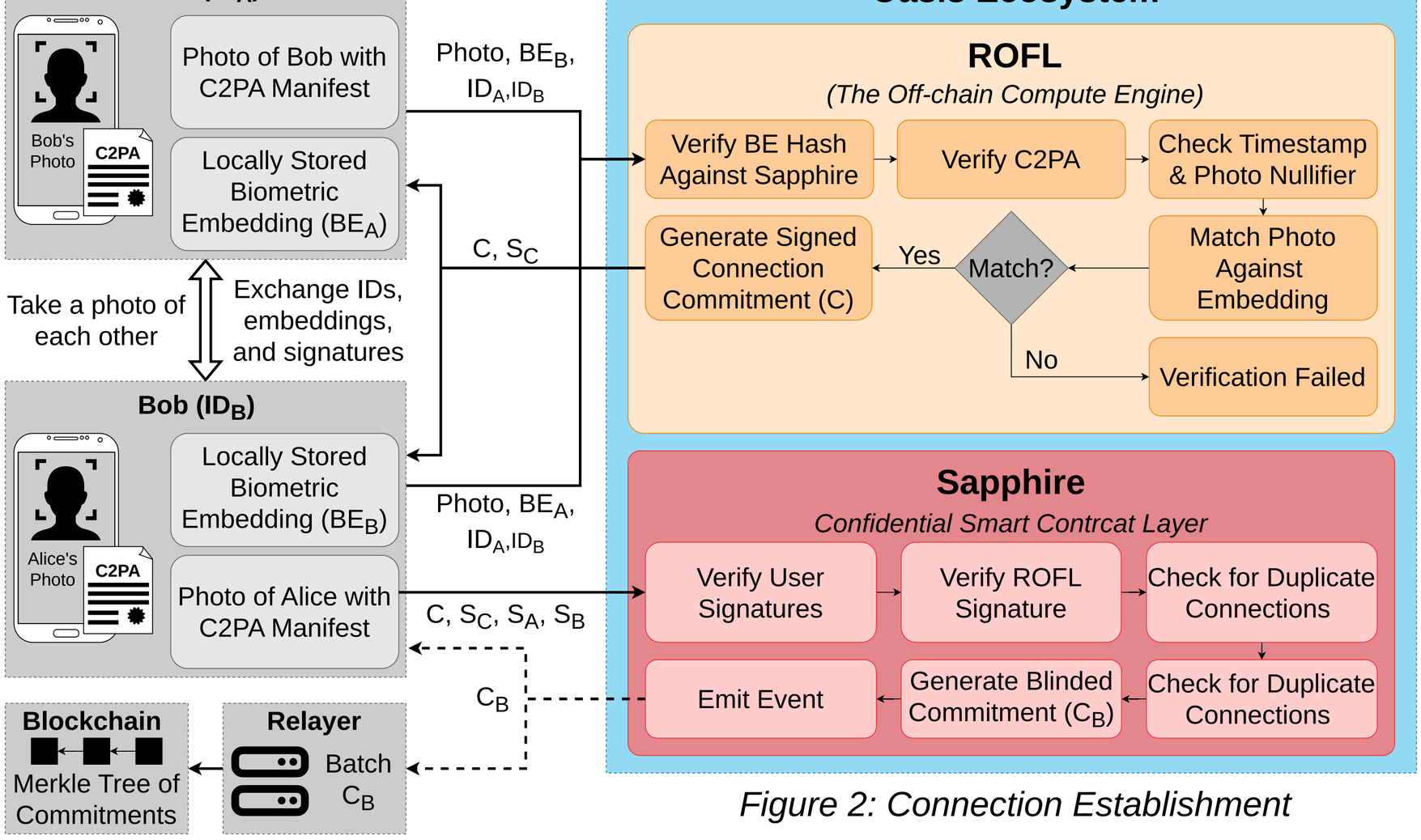
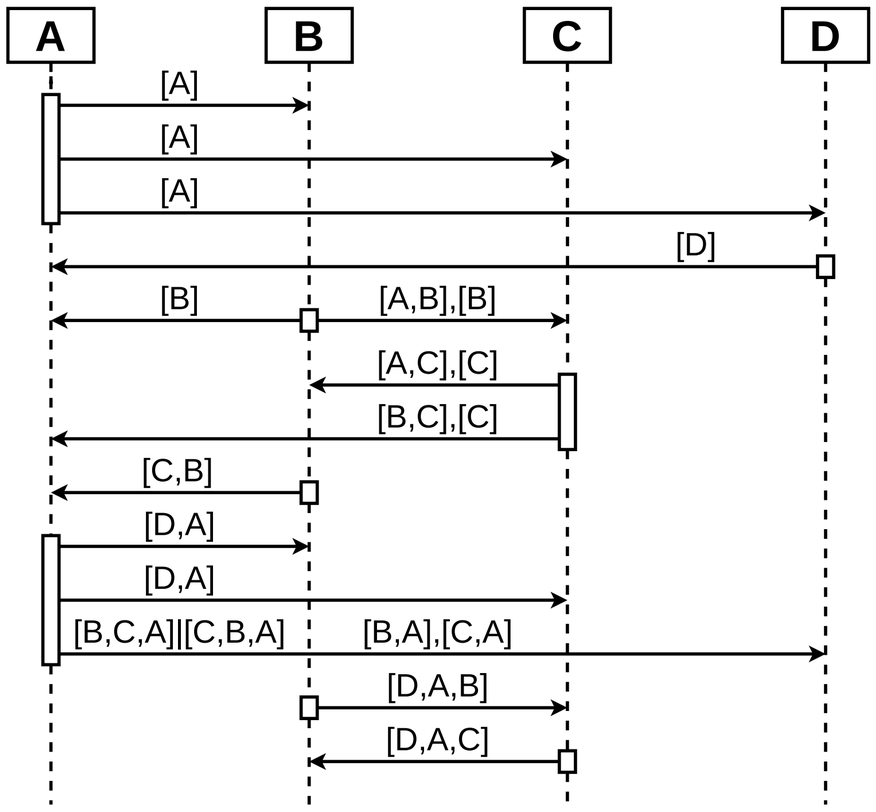


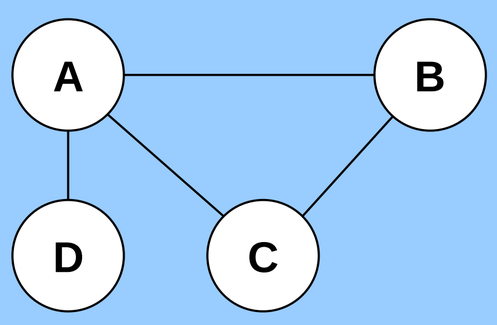
Figure 2: Connection Establishment



Private Random Walks

Using connection commitments, users can generate random walks through a social graph without the graph being centrally stored or revealing individual identities. Each user anonymously proves a connection to another person, sharing these proofs to be used recursively in subsequent steps to extend the path. This process effectively functions as an Incrementally Verifiable Computation (IVC), enabling verifiable discovery across the network while ensuring that each participant knows only their direct connections.

Users must demonstrate multiple paths that do not overlap through the same individuals. This method is based on graph algorithms for Sybil analysis. It assumes that Sybil entities are only weakly connected to the honest portions of the graph. As a result, they cannot obtain enough distinct paths.



The diagram in Figure 3 illustrates the process of gradually creating paths in the graph between four users. The graph connecting these users is shown alongside. Users cannot see this graph; they are only aware of their direct connections. The edges always indicate which path the user is proving in the direction of the arrow.

For example, A initiates a path and sends a proof to B. B uses this proof and sends the path [A,B] to C. Paths through the entire graph are created iteratively. Each path consists of 6 to 8 people, and since there may be many paths, users can choose which ones to follow.