

anoncreds

Samuel Schlesinger

April 15, 2025

An Anonymous Credit Scheme consists of several probabilistic polynomial time algorithms.

1. $(x, w) \leftarrow \text{GenerateKeyPair}$
2. $(p, req) \leftarrow \text{RequestIssuance}$
3. $resp \leftarrow \text{Issue}(x, req, n)$
4. $token \leftarrow \text{IssueCredits}(p, w, req, resp)$
5. $(p, sp) \leftarrow \text{Spend}(token, charge, w)$
6. $refund \leftarrow \text{Refund}(x, sp)$
7. $token \leftarrow \text{RefundCredits}(p, refund, w)$