anoncreds

Samuel Schlesinger

April 15, 2025

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

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

Definition 1. *Double Spend Detection*
(High level) an issuer should be able to detect double spends.

Definition 2. *Fiscal Soundness*
(High level) an issuer should be assured that the total number of credits spent is less than or equal to the total number of credits issued.

Definition 3. *Anonymity*
(High level) clients should be confident that their spends cannot be correlated to their issuances or previous spends with probability better than guessing. In particular, assuming there are multiple unspent credit tokens with greater than or equal to c credits, an issuer should not have any advantage over random chance in guessing which of these tokens were spent.