zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure

Michael Rosenberg, Jacob White, Christina Garman, Ian Miers
{white570,clg}@purdue.edu  {micro,imiers}@umd.edu

What is an Anonymous Credential?
A digital identifier which lets you disclose specific identifying data without revealing or linking others.

Decoupling ID Assurance from Issuance
- Minimize burden of authorizing anonymous credentials & using customized cryptography
- Bootstrap from trusted identity documents
- Zero knowledge (ZK) proofs preserve privacy

Flexible & Auditable Issuance
- Auditable, verifiable issuance of ZK credentials
- Multi issuer, multi application interoperability
- Efficient, dynamic additions to membership list
- Privacy aware list publication and updates

Complex & Composable Statements
- Leverage rich zkSNARK proof framework
- Gadgets: rate limiting, anti cloning, expiry, etc.
- Unlinkable shows of credential between apps

Efficient & Open Source Libraries
- User friendly anonymous credentials API
- Combine & reuse slow proofs (e.g. membership)
- < 150 ms to show, < 5 ms to verify, ~ 1 KB proof size