ZKPs with zk-SNARKs[1][2] in a DIDComm ecosystem

- Berend Sliedrecht, berend@animo.id
- Software Engineer at Animo Solutions

Introduction

In the verifiable credential (VC) space we use zero-knowledge proofs (ZKPs). ZKPs are extremely powerful as they allow a prover to make attestations to a verifier without revealing the underyling value. The classic example is buying alchocol and proving that you are indeed above the age of 18 without revealing your date of birth. Currently, under the AnonCreds (camenisch lysyanskaya signatures) scheme, we can do this on basic predicate operations like `>`, `<`, `==` on values within a credential. BBS+, the other signature scheme that is being used, does not currently support these predicate operations. Operations like these, amongst others, make it possible to support ZKPs.

Why?

zkSNARKs and credentials could enable many new use cases without disclosing more information than required. zkSNARKs allow verifiers to construct complex circuits which can be used by a holder to proof anything about their credentials. This could be a simple predicate asking if `age > 21` or a multi-variable computation whether someone can get a loan.

Research questions

1. What implementation, or variation, of zkSNARKs would fit best within the VC space?
2. Is constructing and executing a circuit efficient enough for a mobile environment?
3. What is the best way to integrate this into the VC ecosystem?
4. A special signature suite?
5. I believe, that the current signatures, CL and BBS+, create proof of knowledge, but zkSNARKs are about argument of knowledge. Will this be an issue?

Resources

- https://z.cash/technology/zksnarks/

[1] Non-interactive zero-knowledge proof

[2] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. 2012. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (ITCS '12). Association for Computing Machinery, New York, NY, USA, 326–349. https://doi.org/10.1145/2090236.2090263

- https://preview.gataca.io/blog/ssi-essentials-which-selective-disclosure-protocol-will-succeed
- https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/