VC-ZKLang

Specification of Privacy-Enhancing Implementation of Verifiable Claims

Jan Camenisch Manu Drijvers ?

30th November 2017

Abstract

This document specifies an language that allow one to describe the cryptographic protocols that will generate a cryptographic token as a witness to a verifiable claim. The cryptographic protocol that will then be executed from this specification should be (but need not be) such that the token is not linkable to the credentials on which it is based.

Contents

1 ZKLang

If credentials are key-bound, they are required to be bound to the same (secret) key.

At this level, all message m_i are integers.

$$\mathrm{NIZK}\{(m_i)_{i \in h}[m]_{i \notin h} : \mathrm{Credential}(\mathit{ipk}, m_1, m_2, m_3)\} \tag{1}$$

$$\mathrm{NIZK}\{() : \mathrm{Nym}(\mathit{nym})\} \tag{2}$$

$$\mathrm{NIZK}\{() : \mathrm{SNym}(\mathit{nym}, \mathit{scope})\} \tag{3}$$

$$\mathrm{NIZK}\{(m) : \mathrm{Enc}(\mathit{epk}, m, \mathit{ctxt})\} \tag{4}$$

$$\mathrm{NIZK}\{(m) : \mathrm{Larger}(m, c)\} \tag{5}$$

$$\mathrm{NIZK}\{(m) : \mathrm{Smaller}(m, c)\} \tag{6}$$

Example composition: here

Explanations of stuff

2 Mapping Verifiable Claims to ZKLang

3 Realization of ZKLang Components

m_i from Z_q, so everything in prime order group

Nyms

CL sigs

Vereng

Orchestration