VC-ZKLang

Specification of Privacy-Enhancing Implementation of Verifiable Claims

Jan Camenisch Manu Drijvers ?

1st December 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. Terms that the language supports are the following ones.

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

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

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

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

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

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

Example composition of a statement.

$$\begin{aligned}&\mathrm{NIZK}\{(m_1, m_2, m_3, m_4)[m_5] : \\ &\qquad \mathrm{Credential}(\mathit{ipk}_1, m_1, m_2, m_3) \ \wedge\ \mathrm{Credential}(\mathit{ipk}_2, m_1, m_4, m_5)\ \wedge \\ &\qquad\qquad\qquad\qquad \mathrm{Nym}(\mathit{nym})\ \wedge\ \mathrm{Larger}(m_3, c)\}\end{aligned}$$

Explanations of stuff

2 Mapping Verifiable Claims to ZKLang

This mapping will depend on the credential specification of the issuer of a credentials.

2.1 Mapping the different types to integers

2.2 Age proof

2.3 Membership proof

3 Realization of ZKLang Components

We could do all of this with X509 credentials, but then have no privacy features. We here concentrate on how to do this with the privacy features.

We assume that the system parameters describe a groups $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, of prime order q, with efficiently computable bilinear map e. We further assume here that all attributes m_i are elements of Z_q, and consider the encoding of other typed attribute values in different sections.

3.1 CL signatures

A credential will take the form of a signature created by an issuer. As we want to prove knowledge of credentials, we need "signatures with efficient protocols", also called CL signatures [CL03]. Examples are the RSA-based CL signature [CL03], the pairing-based CL signature [CL04], and the BBS+ signature scheme [BBS04, ASMC13]. We recall the BBS+ signature scheme:

Key Generation Take $(h_0, \ldots, h_L) \leftarrow \mathbb{G}_1^{L+1}$, $x \leftarrow Z_q^*$, $w \leftarrow g_2^x$, and set $sk = x$ and $pk = (w, h_0, \ldots, h_L)$.

Signature On input message $(m_1, \ldots, m_L) \in Z_q^L$ and secret key x, pick $e, s \leftarrow Z_q$ and compute $A \leftarrow (g_1 h_0^s \prod_{i=1}^{L} h_i^{m_i})^{\frac{1}{e+x}}$. Output signature $\sigma \leftarrow (A, e, s)$.

Verification On input a public key $(w, h_0, \ldots, h_L) \in \mathbb{G}_2 \times \mathbb{G}_1^{L+1}$, message $(m_1, \ldots, m_L) \in Z_q^L$, and purported signature $(A, e, s) \in \mathbb{G}_1 \times Z_q^2$, check $e(A, wg_2^e) = e(g_1 h_0^s \prod_{i=1}^{L} h_i^{m_i}, g_2)$.

We can use the following zero-knowledge proof to prove knowledge of a BBS+ signature, while selectively disclosing the attributes [CDL16]: The prover has signature $\sigma \leftarrow (A, e, s)$ with $A = (g_1 h_0^s \prod_{i=1}^{L} h_i^{m_i})^{\frac{1}{e+x}}$. He can prove knowledge of a BBS+ signature while selectively disclosing messages m_i with $i \in D$. Randomize the credential by taking $r_1 \leftarrow Z_q^*$, set $A' \leftarrow A^{r_1}$, and set $r_3 \leftarrow \frac{1}{r_1}$. Set $\bar{A} \leftarrow A'^{-e} \cdot b^{r_1} (= A'^x)$. Choose $r_2 \leftarrow Z_p$, set $d \leftarrow (g_1 h_0^s \prod_{i=1}^{L} h_i^{m_i})^{r_1} \cdot h_0^{-r_2}$, and set $s' \leftarrow s - r_2 \cdot r_3$. The prover now proves

$$\pi \in SPK\{(\{m_i\}_{i \notin D}, e, r_2, r_3, s') : \\ \bar{A}/d = A'^{-e} \cdot h_0^{r_2} \ \wedge \ g_1 \prod_{i \in D} h_i{}^{m_i} = d^{r_3} h_0^{-s'} \prod_{i \notin D} h_i{}^{-m_i}\}.$$

The resulting proof consists of $(A', \bar{A}, d, \pi)$. To verify a proof, the verifier checks $A' \neq 1_{\mathbb{G}_1}$, $e(A', X) = e(\bar{A}, g_2)$, and verifies π.

3.2 Pseudonyms

Pseudonyms will be formed from Pedersen commitments [Ped92]. Let g_1 and h_1 be generators of $\mathbb{G}_1$.

Commit To commit to a value $m_1 \in Z_q$, take $r \leftarrow Z_q$ and output $c \leftarrow g_1^{m_1} h_1^r$.

ComVf To verify that c commits to m_1 with opening r, check $c \stackrel{?}{=} g_1^{m_1} h_1^r$.

One can efficiently prove that a pseudonym *nym* is correctly constructed by proving

$$\pi \in SPK\{(m_1, r) : nym = g_1^{m_1} h_1^r$$

.

3.3 Range proofs

3.4 Verifiable Encryption

3.5 Orchestration

References

[ASMC13] Man Ho Au, Willy Susilo, Yi Mu, and Sherman S. M. Chow. Constant-size dynamic \$k\$ -times anonymous authentication. *IEEE Systems Journal*, 7(2):249–261, 2013.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matthew K. Franklin, editor, *Advances in Cryptology — CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55. Springer Verlag, 2004.

[CDL16] Jan Camenisch, Manu Drijvers, and Anja Lehmann. Anonymous attestation using the strong diffie hellman assumption revisited. *IACR Cryptology ePrint Archive*, 2016:663, 2016.

[CL03] Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. volume 2576 of *Lecture Notes in Computer Science*, pages 268–289, Amalfi, Italy, September 2003. Springer-Verlag.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. volume 3152 of *Lecture Notes in Computer Science*, pages 56–72, Santa Barbara, CA, USA, August 2004. Springer-Verlag.

[Ped92] Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. volume 576 of *Lecture Notes in Computer Science*, pages 129–140, Santa Barbara, CA, USA, August 1992. Springer-Verlag.