Identrix ZKP

Alexander Nie

August 2018

1 ZKP

For its zkSNARK, Identrix will use a modified version of the Quadratic Spanning Program (QSP) Problem. Briefly, this problem involves taking a set of polynomials $v_i, w_i, t|_{i=1}^{m}$ over a field $\mathbb{F}$ and finding a linear combination of the v and w polynomials which forms a multiple of the target polynomial t. That is, we want to find the elements a_i, b_i of the field $\mathbb{F}$ such that the elements multiplied by the polynomials v_i, w_i give a multiple of t. In mathematical notation,

$$\text{Let } m \in \mathbb{Z} : \forall i, 1 \leq i \leq m, v_i, w_i, t \in \mathbb{F}[x] \tag{1}$$

$$\text{Let } a_i, b_i \in \mathbb{F}, h \in \mathbb{F}[x] \text{ and let } u = \{a_i, b_i\})_{i=1}^{m} \text{ for some choice of } a_i, b_i \tag{2}$$

$$\exists h \in F[x] \text{ and } u : v_a(u)w_b(u) = \left(\sum_{i=1}^{m} a_i v_i\right)\left(\sum_{i=1}^{m} b_i w_i\right) = ht \tag{3}$$

$$\text{Problem: find one such value of } u \tag{4}$$

The QSP problem belongs to a group of problems known as **NP**-complete, which means all other problems in the set **NP** (most cryptography problems) can be rephrased as a QSP using a *reduction function* f which runs in polynomial time. This is important for Identrix because the question "Can Authenticator prove Bob over 25 years old?" can be expressed as a logic circuit for the SAT problem, which is in **NP**, so f allows us to transform this into the QSP question "Can Authenticator show me a combination of a_i, b_i to make the polynomials equal?". The specific reduction function f will depend on the context of the statement to be proved (it will vary by dApp).

Two improvements features distinguish the Identrix ZKP scheme from traditional ZKPs. First, rather than performing polynomial multiplication on the v_i, w_i, an evaluation point x_0 is chosen so the Verifier/Service Provider only needs to check

$$\left(\sum_{i=1}^{m} a_i v_i(x_0)\right)\left(\sum_{i=1}^{m} b_i w_i(x_0)\right) = h(x_0)t(x_0)$$

which is a number rather than an algebraic expression. Second, in the *zero-knowledge* form of the QSP problem, the polynomials are encoded using a homomorphic transformation along an elliptic curve. Essentially, this is a transformation E with the property $E(xy) = E(x)E(y)$ which allows us to encode the test-point x_0 and the polynomials since $E(a_i v_i(x_0)) = a_i v_i(E(x_0))$. A further level of obfuscation is added by multiplying by a random constant α so that the Service Provider cannot figure out the a_i, b_i supplied by the Prover (instead they receive αa_i, αb_i). Then the equality must still hold for the proof to be true:

$$\left(\sum_{i=1}^{m} a_i E(\alpha v_i(x_0))\right)\left(\sum_{i=1}^{m} b_i E(\alpha w_i(x_0))\right) = E(\alpha h(x_0))E(\alpha t(x_0))$$