SchnorrVerdict

We demonstrate a simple gate checker functionality for the equality of the Schnorr Signature,

$$SchnorrVerdict(m, pk, e, s, v)$$

which enforces a field element v (the *verdict*) to reflect verifiable/non-verifiable by Boolean values $1/0$.

EquVerdict: a simple equality verdict

The gadget

$$EquVerdict(x, y, v)$$

enforces that v is a Boolean field element which is 1 if the two field elements x and y are equal, and 0 otherwise.

It allocates a private field elements c and c', and simply enforces

$$\begin{aligned}
x &= v \cdot y + (1 - v) \cdot c \cdot y, \\
0 &= v \cdot (1 - v), \\
1 &= c' \cdot (1 - c).
\end{aligned}$$

Here, the third condition enforces that $c \neq 1$ (otherwise it is not satisfiable), by demanding the existence of a multiplicative inverse (namely, c'), and v (the second equation is the usual Boolean condition for v) is a switch for what the first equation asserts:

- if $v = 1$ the first equation reads $x = y$, hence enforces equality, and
- if $v = 0$ the equation reads $x = c \cdot y$, with $c \neq 1$, hence enforces inequality.

SchnorrVerdict: verdict for signature validity

The gadget $SchnorrVerdict(m, pk, e, s, v)$ implements a circuit in which v as Boolean field element corresponds to the validity of (e, s) with respect to (m, pk), i.e. $v = 1$ if the signature verifies, and $v = 0$ if it NOT verifies.

We demonstrate it's construction using the length-restricted version of the Schnorr Signature (as in SchnorrSignature.md).

The circuit just a slight modification of $SchnorrVerify(m, pk, e, s)$, but allowing to be satisfiable even when the signature does not verify (but always forcing to encode that fact in the verdict v). As in $SchnorrVerify$ we consider m as single F-element , load both e and s as F elements e_F and s_F, allocate private F-elements $(e_i)_{i=0}^{L-2}$, $(s_i)_{i=0}^{L-2}$, private elliptic curve points R, U, V from $\mathbb{G} = EC(F)$, and enforce that

$$\begin{aligned}
0 &= e_i \cdot (e_i - 1), \qquad & 0 &= s_i \cdot (s_i - 1), \qquad & i &= 0, 1, \ldots, L-2, \\
e_F &= \sum_{i=0}^{L-2} e_i \cdot 2^i, \qquad & s_F &= \sum_{i=0}^{L-2} s_i \cdot 2^i,
\end{aligned}$$

as well as

$$
\begin{aligned}
U &= ECadd(V, R) \\
U &= SquareAndMultiply(G, (s_i)_{i=0}^{L-2}), \\
V &= SquareAndMultiply(pk, (e_i)_{i=0}^{L-2}),
\end{aligned}
$$

and finally use $EquVerdict$ to enforce v to encode the fact whether e_F equals $PH_F(m, pk, R)$ of not:

$$
EquVerdict(e_F,PH_F(m,pk,R),v).
$$

$$EquVerdict(e_F, PH_F(m, pk, R), v).$$

$$EquVerdict(e_F, PH_F(m, pk, R), v).$$