Writing circuits

circom allows programmers to define theconstraints that define the arithmetic circuit. All constraints must be of the form A*B + C = 0, where A, B and C are linear combinations of signals. More details about these equations can be foundhere .

The arithmetic circuits built usingcircom operate on signals. Let us define our first circuit that simply multiplies two input signals and produces an output signal.

```
pragma circom 2.0.0;

/*This circuit template checks that c is the multiplication of a and b*/

template Multiplier2 () {

// Declaration of signals.
signal input a;
signal input b;
signal output c;

// Constraints.
c <== a * b;
}
```

First, thepragma instruction is used to specify the compiler version. This is to ensure that the circuit is compatible with the compiler version indicated after thepragma instruction. Otherwise, the compiler will throw a warning.

Then, we use the reserved keywordtemplate to define the shape of a new circuit, calledMultiplier2 . Now, we have to define itssignals . Signals can be named with an identifier, e.g.,a, b, c. In this circuit, we have two input signalsa, b and an output signalc . Finally, we use<== to set that the value ofc is the result of multiplying the values ofa andb . Equivalently, we could have also used the operator==> , e.g.,a * b ==> c .

Let us notice that in each template, we first declare its signals, and after that, the associated constraints.