Status of CFRG curves

agl

Goldilocks has been included.

- Algorithms have been tweaked to work with the different length.
- I’ve not re-checked them yet.

Sending u-value for DH

- No changes to the draft needed—it already did that.

Checking for zero output.

- Happens when the point input has the wrong order.
- Checking is very cheap
- It’s now a MUST.

Parameter generation

- We used to generate (twisted) Edwards curves and then hop isomorphisms and isogenies to get where we needed.
- We now generate Montgomery curves directly. We can hop to (twisted) Edwards for signatures if that happens.

SAGE, not pseudocode.

- You can now execute the code in the draft with SAGE and reconfirm the curves.
- It’ll take a while.
- I haven’t finished yet.

Base points

- We specify an algorithm for generating base points again.
- It’s in SAGE.
- It generates the standard base point for curve25519 and u=5 for curve448.