Spiral (or Skip) Ratchet

A Backwards-Secret Positional Numeral System

Brooklyn Zelenka
Fission Codes
brooklyn@fission.codes

December 7, 2021

Abstract

This a great program for writing math. I can write in line math and other stuff

1 Ratchet

The basic idea for cryptographic ratchets is that repeatedly hashing a value creates a kind of backwards-secret clock. When you start watching the clock, you can generate the hash for any arbitrary future steps, but not steps from prior to observation since that requires computing the SHA3 preimage.

SHA3-256 is native to the WebCypto API, is a very fast operation, and commonly hardware accelerated. Anecdotally, Firefox on an Apple M1 completes each SHA3 3µs (100k/300ms). The problem with a single hash counter is threefold: