I’m wondering if my line of thinking is correct. Construct an accumulator, which resembles a Merkle tree, but non-leaf nodes are XOR’ed, rather than hashed. Publish the root, and proofs of items are worst-case O(log N) long.

This is not an original idea, it’s been specifically brought up here in the zcash repo and also referred to in general about alternatives to Merkle accumulators.