Explicit Optimal Binary Pebbling for One-Way Hash Chain Reversal

One-way hash chains form a fundamental construct in cryptography. As (part of an) authentication mechanism, the basic idea is to first generate a hash chain by iterating a cryptographic hash function such as SHA-256, given a seed as starting value, and then later to release the elements of the hash chain in reverse order. The elements are released one element at a time in successive rounds. Due to the one-way property of the hash function, however, reversal of such a one-way hash chain is non-trivial for very long chains (say of length $n = 2^{32}$) if one limits the amount of storage to $O(\log n)$ as well as the running time per round to $O(\log n)$. This problem was first studied by Coppersmith and Jakobsson in 2002, who achieved almost optimal results. In this talk, we present a simple general framework for efficient binary reversal algorithms, and we provide the first explicit optimal solution.