Cryptology ePrint Archive: Report 2011/102

Cryptography for Efficiency: Authenticated Data Structures Based on Lattices and Parallel Online Memory Checking

Charalampos Papamanthou and Roberto Tamassia

Abstract: In this work, we initially design a new authenticated data structure for a \emph{dynamic table} with n entries. We present the first dynamic authenticated table that is \emph{update-optimal}, using a \emph{lattice-based} construction. In particular, the update complexity is $O(1)$, improving in this way the ``a priori'' $O(\log n)$ update bounds of previous constructions, such as the Merkle tree. Moreover, the space complexity of our authenticated data structure is $O(n)$ and logarithmic bounds hold for other performance measures, such as proof complexity (number of group elements contained in the proof). To achieve this result, we establish and exploit a property that we call \emph{repeated linearity} of lattice-based hash functions and show how the security of lattice-based digests can be guaranteed under updates. An one-time preprocessing stage of $O(n\log n)$ complexity is also required at setup. This is the first construction achieving a constant update bound without causing other complexities to increase beyond logarithmic. All previous solutions enjoying such a complexity bound for updates enforce $\Omega(n^\epsilon)$ proof or query complexity. As an application, we provide the first construction of an authenticated Bloom filter, an update-intensive data structure that falls into our model.

We secondly observe that the repeated linearity of the used lattice-based cryptographic primitive lends itself to a natural notion of parallelism: As such, we describe \emph{parallel} versions of our authenticated data structure algorithms, yielding the first parallel \emph{online memory checker} with $O(1)$ query complexity using $O(\log n)$ checkers in the CREW model and without using a secret key setting, i.e., there is only need for small \emph{reliable} but not \emph{secret} memory. We base the security of our constructions on the difficulty of approximating the gap version of the shortest vector problem in lattices (GAPSVP) within polynomial factors.

Category / Keywords: authenticated data structures, lattice-based cryptography, memory checking

Date: received 1 Mar 2011, last revised 3 Mar 2011

Contact author: cpap at cs brown edu

Available formats: PDF | BibTeX Citation

Version: 20110303:203617 (All versions of this report)