Cryptology ePrint Archive: Report 2015/227

Tradeoff Cryptanalysis of Memory-Hard Functions

Alex Biryukov and Dmitry Khovratovich

Abstract: We explore time-memory and other tradeoffs for memory-hard functions, which are supposed to impose significant computational and time penalties if less memory is used than intended. We analyze three finalists of the Password Hashing Competition: Catena, which was presented at Asiacrypt 2014, \textsf{yescrypt} and Lyra2. We demonstrate that Catena's proof of tradeoff resilience is flawed, and attack it with a novel \emph{precomputation tradeoff}. We show that using $M^{4/5}$ memory instead of M we have no time penalties and reduce the AT cost by the factor of 25. We further generalize our method for a wide class of schemes with predictable memory access. For a wide class of data-dependent schemes, which addresses memory unpredictably, we develop a novel \emph{ranking tradeoff} and show how to decrease the time-memory and the time-area product by significant factors. We then apply our method to yescrypt and Lyra2 also exploiting the iterative structure of their internal compression functions. The designers confirmed our attacks and responded by adding a new mode for Catena and tweaking Lyra2.

Category / Keywords: password hashing, memory-hard, Catena, tradeoff, cryptocurrency, proof-of-work

Original Publication (in the same form): IACR-ASIACRYPT-2015

Date: received 10 Mar 2015, last revised 28 Sep 2015

Contact author: alex biryukov at uni lu; khovratovich@gmail com

Available format(s): PDF | BibTeX Citation

Version: 20150928:102957 (All versions of this report)

Short URL: ia.cr/2015/227

[Cryptology ePrint archive]