Cryptology ePrint Archive: Report 2011/665

Efficient Modular Exponentiation-based Puzzles for Denial-of-Service Protection

Jothi Rangasamy \and Douglas Stebila \and Lakshmi Kuppusamy \and Colin Boyd \and Juan Gonzalez Nieto

Abstract: Client puzzles are moderately-hard cryptographic problems --- neither easy nor impossible to solve --- that can be used as a countermeasure against denial of service attacks on network protocols. Puzzles based on modular exponentiation are attractive as they provide important properties such as non-parallelisability, deterministic solving time, and linear granularity. We propose an efficient client puzzle based on modular exponentiation. Our puzzle requires only a few modular multiplications for puzzle generation and verification. For a server under denial of service attack, this is a significant improvement as the best known non-parallelisable puzzle proposed by Karame and \v{C}apkun (ESORICS 2010) requires at least $2k$-bit modular exponentiation, where k is a security parameter. We show that our puzzle satisfies the unforgeability and difficulty properties defined by Chen \etal{} (Asiacrypt 2009). We present experimental results which show that, for 1024-bit moduli, our proposed puzzle can be up to $30 \times$ faster to verify than the Karame-\v{C}apkun puzzle and $ 99 \times$ faster than the Rivest \etal's time-lock puzzle.

Category / Keywords: client puzzles, time-lock puzzles, denial of service resistance, RSA, puzzle difficulty

Date: received 8 Dec 2011

Contact author: j rangasamy at qut edu au