Cryptology ePrint Archive: Report 2013/175

Machine-Generated Algorithms, Proofs and Software for the Batch Verification of Digital Signature Schemes

Joseph A. Akinyele and Matthew Green and Susan Hohenberger and Matthew W. Pagano

Abstract: As devices everywhere increasingly communicate with each other, many security applications will require low-bandwidth signatures that can be processed quickly. Pairing-based signatures can be very short, but are often costly to verify. Fortunately, they also tend to have efficient batch verification algorithms. Finding these batching algorithms by hand, however, can be tedious and error prone.

We address this by presenting AutoBatch, an automated tool for generating batch verification code in either Python or C++ from a high level representation of a signature scheme. AutoBatch outputs both software and, for transparency, a LaTeX file describing the batching algorithm and arguing that it preserves the unforgeability of the original scheme.

We tested AutoBatch on over a dozen pairing-based schemes to demonstrate that a computer could find competitive batching solutions in a reasonable amount of time. Indeed, it proved highly competitive. In particular, it found an algorithm that is significantly faster than a batching algorithm from Eurocrypt 2010. Another novel contribution is that it handles cross-scheme batching, where it searches for a common algebraic structure between two distinct schemes and attempts to batch them together.

In this work, we expand upon an extended abstract on AutoBatch appearing in ACM CCS 2012 in a number of ways. We add a new loop-unrolling technique and show that it helps cut the batch verification cost of one scheme by roughly half. We describe our pruning and search algorithms in greater detail, including pseudocode and diagrams. All experiments were also re-run using the RELIC pairing library. We compare those results to our earlier results using the MIRACL library, and discuss why RELIC outperforms MIRACL in all but two cases. Automated proofs of several new batching algorithms are also included.

AutoBatch is a useful tool for cryptographic designers and implementors, and to our knowledge, it is the first attempt to outsource to machines the design, proof writing and implementation of signature batch verification schemes.

Category / Keywords: implementation / digital signatures, pairing-based cryptography, batch verification, automation, crypographic compiler

Publication Info: ACM CCS 2012

Date: received 27 Mar 2013

Contact author: akinyelj at cs jhu edu