BATCH VERIFICATION OF ELLIPTIC CURVE AND EDWARDS CURVE DIGITAL SIGNATURES

Sabyasachi Karati

BATCH VERIFICATION OF ELLIPTIC CURVE AND EDWARDS CURVE DIGITAL SIGNATURES

Thesis submitted in partial fulfillment
of the requirements for the award of the degree

of

Doctor of Philosophy

by

Sabyasachi Karati

Under the supervision of

Dr. Abhijit Das

Department of Computer Science and Engineering

Indian Institute of Technology, Kharagpur

2014

ABSTRACT

In this thesis, several algorithms for the batch verification of standard ECDSA signatures are introduced. The first of these algorithms is based upon the naive idea of taking square roots in the underlying field. In order to improve the efficiency beyond what can be achieved by the naive algorithm, two new algorithms are initially proposed, which replace square-root computations by symbolic manipulations. We then use elliptic-curve summation polynomials to design ECDSA batch-verification algorithms which are significantly faster than our batch-verification algorithms based on symbolic manipulations. Experiments carried out on NIST prime curves demonstrate a maximum speedup of above six over individual verification if all the signatures in the batch belong to the same signer, and a maximum speedup of about two if the signatures in the batch belong to different signers, both achieved by a fast variant of our batch-verification algorithm based on elliptic-curve summation polynomials. We also establish a theoretical connection between our symbolic-computation and summation-polynomial algorithms. To the best of our knowledge, these are the first algorithms to address the problem of batch verification of standard ECDSA signatures.

We propose three randomization methods for our batch-verification algorithms in order to prevent several types of attacks. The first method is based on Montgomery ladders, and the second on computing square roots in the underlying field. Both these methods use numeric arithmetic only. Our third proposal exploits symbolic computations leading to a seminumeric algorithm. We theoretically and experimentally prove that for standard ECDSA signatures, our seminumeric randomization algorithm in tandem with the summation-polynomial-based batch-verification algorithm gives the best speedup over individual verification. If each ECDSA signature contains an extra bit to uniquely identify the correct y-coordinate of the elliptic-curve point appearing in the signature, then the second (numeric) randomization method followed by the naive batch-verification algorithm yields the best performance gains. Randomization significantly brings down the performance gains achieved by batch verification. For standard ECDSA signatures, our experiments reveal a maximum reduced speedup close to two for half-length

randomizers and for all signatures in a batch coming from the same signer.

We theoretically prove that all the proposed algorithms offer the same security as the straightforward batch verification of ECDSA* signatures in which the x-coordinates of the elliptic-curve points are replaced by the entire points.

Our batch-verification algorithms are also ported to NIST Koblitz curves defined over finite fields of characteristic two. We also make a comparative study of our algorithms for the Edwards curve digital signature algorithm (EdDSA) over a medium-sized prime field. We report our experimental results both with and without randomization.

All our algorithms are practical only for small ($\leqslant 10$) batch sizes, because their running times and space requirements are exponential in the batch size. It remains an open problem whether the batch-verification problem for standard ECDSA signatures can be solved in less than exponential (possibly even in polynomial) time.

Keywords: Digital Signatures, Elliptic Curves, Koblitz Curve, Edwards Curve, ECDSA, EdDSA, Batch Verification, Scalar Multiplication, Symbolic Computation, Linearization, Multivariate Polynomial, Summation Polynomial, Randomization, Montgomery Ladder