Performance Analysis of Pairing-Based Elliptic Curve Cryptography on Constrained Devices

Submitted by aekwall on Wed, 05/01/2019 - 11:38am

Title	Performance Analysis of Pairing-Based Elliptic Curve Cryptography on Constrained Devices
Publication Type	Conference Paper
Year of Publication	2018
Authors	Hajny, J., Dzurenda, P., Ricci, S., Malina, L., Vrba, K.
Conference Name	2018 10th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)
Keywords	Bilinear Pairing, bilinear pairing operation, Constrained Devices, cryptographic libraries, cryptographic protocols, cryptography, digital signatures, Elliptic curve cryptography, Elliptic curves, embedded devices, group signatures, identity-based encryption schemes, Metrics, pairing-based elliptic curve cryptography, performance evaluation, pubcrawl, public key cryptography, Resiliency, Scalability, smart cards, smart meters, Standards, Telecommunications

Abstract

The paper deals with the implementation aspects of the bilinear pairing operation over an elliptic curve on constrained devices, such as smart cards, embedded devices, smart meters and similar devices. Although cryptographic constructions, such as group signatures, anonymous credentials or identity-based encryption schemes, often rely on the pairing operation, the implementation of such schemes into practical applications is not straightforward, in fact, it may become very difficult. In this paper, we show that the implementation is difficult not only due to the high computational complexity, but also due to the lack of cryptographic libraries and programming interfaces. In particular, we show how difficult it is to implement pairing-based schemes on constrained devices and show the performance of various libraries on different platforms. Furthermore, we show the performance estimates of fundamental cryptographic constructions, the group signatures. The purpose of this paper is to reduce the gap between the cryptographic designers and developers and give performance results that can be used for the estimation of the implementability and performance of novel, upcoming schemes.

URL https://ieeexplore.ieee.org/document/8631228

DOI 10.1109/ICUMT.2018.8631228
Citation Key hajny_performance_2018

Bilinear Pairing bilinear pairing operation Constrained Devices cryptographic libraries Cryptographic Protocols Cryptography digital signatures Elliptic curve cryptography Elliptic curves embedded devices group signatures identity-based encryption schemes Metrics pairing-based elliptic curve cryptography performance evaluation pubcrawl public key cryptography Resiliency Scalability smart cards smart meters standards Telecommunications