Instituto de Computação
Universidade Estadual de Campinas

# Implementação Eficiente em Software de Criptossistemas de Curvas Elípticas

**Julio César López Hernández**

28 de Abril de 2000

**Banca Examinadora:**

- Prof. Dr. Ricardo Dahab
  Universidade Estadual de Campinas (Orientador)
- Prof. Dr. Guido C. S. Araújo
  Universidade Estadual de Campinas
- Prof. Dr. Cláudio L. Lucchesi
  Universidade Estadual de Campinas
- Prof. Dr. Daniel Panario
  Universidade de São Paulo
- Prof. Dr. Routo Terada
  Universidade de Toronto

# Abstract

It is widely recognized that public-key cryptography is an important tool for providing security services such as confidentiality, data integrity, authentication and non-repudiation, which are requirements present in almost all communications. The main advantage of elliptic curve cryptography (ECC) over competing public-key technologies such as RSA and DSA, is that significantly smaller parameters can be used in ECC, but with equivalent levels of security. This advantage is especially important for applications on constrained environments such as smart cards, cell phones, personal device assistants, and pagers.

From a practical point of view, the implementation of ECC presents various challenges. An ECC-based application requires that several choices be made including the security level, algorithms for implementing the finite field arithmetic, algorithms for implementing the elliptic group operation, elliptic curve protocols, and the computer platform. These choices may have a significant impact on the performance of the resulting application.

This dissertation focuses on developing efficient algorithms for software implementation of ECC over $\mathbb{F}_{2^m}$. In this framework, we study different ways of efficiently implementing arithmetic in $\mathbb{F}_{2^m}$, and computing an elliptic scalar multiplication, the central operation of public-key cryptography based on elliptic curves. We also concentrate on the software implementation of these algorithms for different platforms including PCs, workstations, and constrained devices such as the RIM interactive pager.

This dissertation is a collection of five papers written in English, with an introduction and conclusions written in Portuguese.