

ABSTRACT

COMPARATIVE ANALYSIS OF MULTI-PRECISION ARITHMETIC LIBRARIES FOR PUBLIC KEY CRYPTOGRAPHY

Ashraf Abusharekh, M.Sc.
George Mason University, 2004
Thesis Director: Prof. Kris Gaj

Software implementations of Public Key Schemes require efficient realization of operations on large integers and elements of the Galois Field. Typical operand sizes used in public key cryptography range from 768 to 2048 bits for schemes based on large integers, and from 140 to 240 for schemes based on operations in the Galois Field. Multiple libraries implementing such operations exist both commercially and in the public domain, but no study has been done to date to compare and contrast such libraries against each other.

In this thesis we perform comparison of eight multi-precision libraries using criteria such as performance, support of Public Key primitive operations, ease of use, and portability. The performance of all libraries is ranked based on the measurements performed according to the original methodology that takes into account the performance and relative use of primitive cryptographic operations.

The aim of this study is to evaluate the suitability of the investigated libraries for implementation of a wide range of Public Key Cryptosystems such as RSA, DSA and Elliptic Curve Schemes. Practical recommendation regarding the optimum choice of the multi-precision library, depending on the required performance, as well as time and resources devoted to the implementation, are provided.