Capítulo 1

Introducción

Los sistemas criptográficos basados en curvas elípticas fueron propuestos por vez primera de manera independiente por Miller [68] y Koblitz [49], después del trabajo de Lenstra [56] en factorización de enteros. La característica principal de los criptosistemas de curvas elípticas (CCE) es la menor longitud de claves en relación al RSA [82] así como a otros sistemas basados en el logaritmo discreto sobre campos finitos. Se pueden construir sistemas criptográficos basados en el logaritmo discreto sobre curvas elípticas con longitudes de clave de 150 a 200 bits [64]. Actualmente se encuentra en proceso la estandarización de los CCE por la IEEE [52] así como por otros organismos tales como ANSI [4] e ISO [45]. Los CCE pueden servir de base para varios servicios de seguridad tales como el intercambio de claves, privacidad mediante cifrado, y autenticación e integridad de mensajes mediante firmas digitales [32]. Por las razones expuestas los CCE son crecientemente utilizados en aplicaciones de seguridad informática. Por lo tanto, resulta de especial interés el tener implementaciones eficientes de CCE.

Por otro lado, el paralelismo parece ser la alternativa más viable para aumentar la capacidad de procesamiento de las computadoras en un futuro cercano [44] [41] [11]. La posibilidad de construir multicomputadoras a partir de componentes comúnes, en arquitecturas de tipo *Beowulf* [11] así como la existencia de software libre para el desarrollo de aplicaciones de programación paralela ha hecho que se popularice el uso del paralelismo.

Hasta ahora sin embargo, el uso del paralelismo en criptología se ha restringido a la búsqueda de colisiones en paralelo [27] [103] para el criptoanálisis de sistemas basados en logaritmos discretos. Por ejemplo, no existen a la fecha sistemas de criptografía de clave pública que hayan sido especialmente desarrollados para arquitecturas multiprocesadores. La investigación

de algoritmos para exponenciación discreta, operación básica en la mayoría de los sistemas de criptografía de clave pública, se centra exclusivamente en el caso secuencial [104]. Estos algoritmos son de complejidad lineal, aproximadamente, sobre el número de bits del exponente. Es de esperarse entonces que, utilizando procesamiento paralelo, puedan encontrarse algoritmos para exponenciación discreta cuya complejidad sea logarítmica sobre la longitud de la clave. Esto permitiría la creación de sistema de criptografía de clave pública para arquitecturas multiprocesadores.

En este trabajo se presenta un algoritmo para la evaluación de potencias de puntos sobre curvas elípticas que haciendo uso del paralelismo logra reducir el tiempo de ejecución respecto a los algoritmos secuenciales conocidos hasta ahora. Se evalua el desempeño de la implementación del algoritmo sobre una multicomputadora de componentes comunes comparandola con implementaciones en software de CCE reportadas en la literatura y se muestra que el algoritmo es particularmente eficiente en el caso de las curvas de Koblitz. Los resultados mencionados han sido previamente presentados en [35] y [36].