E199

ARITMÉTICA DE CORPOS FINITOS OTIMIZADA PARA CRIPTOGRAFIA DE CURVAS ELÍPTICAS

Alberto Alexandre Assis Miranda (Bolsista PIBIC/CNPq) e Prof. Dr. Ricardo Dahab (Orientador), Instituto de Computação – IC, UNICAMP

A criptografia de chave pública é uma tecnologia imprescindível no provimento de requisitos de segurança em áreas como comunicação pessoal, comércio eletrônico e mais recentemente validade de documentos eletrônicos. Dentre os métodos existentes, um dos mais importantes é o baseado no grupo aditivo dos pontos de uma curva elíptica definida sobre corpos finitos GF(p^n). A eficiência das implementações de tal sistema depende diretamente do desempenho dos algoritmos da aritmética do corpo sobre o qual ele é definido. Este projeto implementou uma biblioteca em C para corpos finitos otimizada para criptografia de curvas elípticas. Como são poucas as restrições na escolha do corpo sobre o qual a curva é definida, há um grande grau de liberdade para se otimizar as implementações em determinadas classes de corpos. As aritméticas das seguintes classes de corpos finitos, interessantes do ponto de vista computacional, foram implementadas: - Corpos com características pouco menores do que a palavra do processador. - Corpos cujo grau n seja pouco menor do que uma potência de 2, para métodos Karatsuba e FFT. - Corpos cuja característica tenha raízes 2^k-ésimas de 1, k=log(n), para possibilitar o uso da FFT. As implementações obtidas fazem parte de um pacote completo de criptografia de curvas elípticas que está sendo implementado por este bolsista, o que inclui procedimentos para escolha de curvas e protocolos de ciframento e assinaturas digitais.

Criptografia - Curvas elípticas - Implementação eficiente