XIII Congresso 28 a 29 - setembro - 2005
Interno de Iniciação Científica da UNICAMP
Ginásio Multidisciplinar da UNICAMP

T841

OTIMIZAÇÃO DE SISTEMAS DE CRIPTOGRAFIA DE CHAVE PÚBLICA BASEADOS EM CURVAS ELÍPTICAS

Mariana Coelho de Oliveira (Bolsista PIBIC/CNPq) e Prof. Dr. Marco Aurélio Amaral Henriques (Orientador), Faculdade de Engenharia Elétrica e de Computação - FEEC, UNICAMP

Com o aumento do uso de sistemas embarcados de computação, tais como telefones celulares e smart-cards, torna-se cada vez mais importante a autenticação de usuários e a proteção das informações armazenadas e/ou trocadas por eles. Isto pode ser feito com recursos de criptografia, que podem ser muito dispendiosos. Este trabalho visa otimizar as operações aritméticas básicas envolvidas na implementação em processador digital de sinais de um sistema de criptografia baseado em curvas elípticas, de forma a tirar o maior proveito possível desta plataforma que tem restrições em poder de processamento e memória, mas pode executar multiplicações com rapidez. Partiu-se de uma infraestrutura de software implementada num trabalho anterior usando corpos de extensão ótima, os quais oferecem uma maior eficiência espacial (menor consumo de memória) e temporal (maior rapidez). Procurou-se, inicialmente, otimizar a rotina de redução modular *(mod p)*, que é a mais recorrente no criptossistema, e tem impacto direto no tempo da rotina de multiplicação de elementos do corpo de extensão ótima. Os resultados obtidos mostram, para esta rotina de multiplicação, redução de até 37,6% no espaço de armazenamento e de até 35,2% no tempo de processamento em relação ao trabalho de referência de multiplicação. Estima-se que reduções ainda mais acentuadas poderão ser obtidas com novas otimizações em outras operações básicas.

Criptografia - Curvas elípticas - Corpos de extensão ótima