T530

IMPLEMENTAÇÃO DE UM SISTEMA DE CRIPTOGRAFIA DE CHAVE PÚBLICA BASEADO EM CURVAS ELÍPTICAS SOBRE CORPOS DE EXTENSÃO ÓTIMA

David R. F. dos Reis Jr. (Bolsista PIBIC/CNPq), Arnaldo J. de Almeida Jr. (CESET-UNICAMP) 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, tornou-se mais importante a autenticação e a proteção do teor das informações armazenadas e/ou trocadas por eles, o que pode ser obtido por meio da criptografia de chave pública. Este tipo de criptografia requer uma quantidade de memória e de poder computacional normalmente não disponíveis em sistemas embarcados. Para tratar deste problema, este trabalho implementa a infraestrutura de software necessária para um sistema de criptografia de chave pública com curvas elípticas baseadas em corpos de extensão ótima, o qual se caracteriza por uma maior eficiência espacial (menor consumo de memória) e temporal (maior rapidez). O sistema desenvolvido foi portado para um Processador de Sinais Digitais (DSP) tipicamente encontrado em telefones celulares e apresentou características de desempenho promissoras, devido à exploração de recursos específicos deste tipo de processador. Pelos resultados obtidos, constata-se a adequação das curvas elípticas baseadas em corpos de extensão ótima para a implementação de criptografia de chave pública em sistemas embarcados.

Criptografia – Curvas Elípticas - Corpos de Extensão Ótima