IX congresso interno de iniciação científica da unicamp
27 e 28 de setembro 2001

ALGORITMOS DE CRIPTOGRAFIA BASEADOS EM CURVAS ELÍPTICAS: IMPLEMENTAÇÃO EM AMBIENTES COMPUTACIONAIS RESTRITOS

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

Quando implementados adequadamente, os algoritmos de criptografia assimétrica com curvas elípticas podem oferecer um nível de segurança superior ao dos métodos convencionais para um mesmo tamanho de chave. Isto significa que é possível implementar criptossistemas baseados em curvas elípticas que ofereçam as mesmas garantias contra quebra de sigilo que outros algoritmos de criptografia assimétrica, mas com chaves menores. Esta característica é bastante atraente sob o ponto de vista da implementação de criptografia em ambientes de computação restrita (como telefones celulares, cartões inteligentes, entre outros) já que um número menor de bits da chave facilita tal implementação e reduz custos de produção, ao mesmo tempo que oferece a segurança de um sistema de criptografia de maior porte. Este trabalho descreve a implementação de algoritmos de criptografia baseados em curvas elípticas em um sistema de processamento digital de sinais (DSP) de ponto fixo como aqueles empregados em telefones celulares digitais. Os algoritmos formam uma plataforma estruturada organizada em camadas que têm funções bem definidas, provendo uma grande flexibilidade ao desenvolvimento e testes de diferentes formas de se empregar as curvas elípticas em criptografia.

Criptografia - Curvas Elípticas - Ambientes Computacionais Restritos