T584

IMPLEMENTAÇÃO EFICIENTE DE SISTEMA DE CODIFICAÇÃO E AUTENTICAÇÃO DE DADOS BASEADO EM CRIPTOGRAFIA DE CHAVE PÚBLICA COM CURVAS ELÍPTICAS

Loreno Ribeiro do Val (Bolsista SAE/PRG), Prof. Arnaldo J. de Almeida Jr. e Prof. Dr. Marco Aurélio Amaral Henriques (Orientador), Faculdade de Engenharia Elétrica e de Computação - FEEC, UNICAMP

É crescente a demanda por sistemas de segurança que protejam e/ou autentiquem a transmissão de dados em plataformas computacionalmente restritas, tais como computadores de mão (palmtops), telefones celulares, smartcards, dentre outras. Este trabalho visa a determinação de formas eficientes de implementar um sistema de codificação e autenticação de dados baseado em uma combinação de algoritmos de criptografia simétrica (Advanced Encryption Standard - AES) e assimétrica (Elliptic Curve Cryptography - ECC) em um processador digital de sinais (DSP) voltado para aplicações portáteis. Neste sistema, a criptografia assimétrica é usada para garantir a autenticidade dos dados e para viabilizar a troca segura de chaves de sessão a serem usadas na codificação dos dados pela criptografia simétrica. O algoritmo baseado em ECC foi escolhido por requerer um tamanho de chave reduzido, quando comparado ao RSA, algoritmo de chave pública mais usado atualmente. O AES foi escolhido por ser um novo padrão para criptografia simétrica e por demandar também poucos recursos computacionais. O sistema de codificação e autenticação resultante mostrou-se adequado para proteger e autenticar as comunicações entre plataformas restritas baseadas em DSP, devido ao seu bom desempenho e baixo consumo de memória.

Criptografia - Chave Pública - Curvas Elípticas