T0945

CRIPTOSSISTEMAS BASEADOS EM EMPARELHAMENTOS BILINEARES SOBRE CURVAS ELÍPTICAS

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

Emparelhamentos bilineares sobre curvas elípticas são funções matemáticas com propriedades que os tornam de interesse para aplicações criptográficas, conforme descoberto recentemente. Os criptossistemas baseados em emparelhamentos bilineares possibilitam a implementação eficiente de protocolos para codificação e autenticação de dados. Tais sistemas são mais eficientes que os esquemas tradicionais de criptografia de chave pública, tornando viável sua aplicação em ambientes computacionais restritos, como celulares. Utilizando a linguagem de programação C, foram implementadas todas as camadas de software necessárias para o cálculo de emparelhamentos bilineares: representação de inteiros grandes, aritmética em corpos binários, operações em curvas elípticas, aritmética em corpos de extensão e, por fim, o próprio emparelhamento. A partir dessa base, foram implementados sistemas de assinatura digital curta, além de esquemas de cifragem e assinatura baseados em identidades. Os criptossistemas implementados apresentaram um funcionamento correto e um bom desempenho quando submetidos a variados tipos de teste, o que permite vislumbrar sua aplicabilidade em servidores, computadores pessoais e dispositivos como celulares e palms.

Criptografia - Curvas elípticas - Emparelhamentos bilineares