T0929

IMPLEMENTAÇÃO E ANÁLISE DE ALGORTIMOS PARA CÁLCULO DE EMPARELHAMENTOS BILINEARES SOBRE CURVAS ELÍPTICAS E HIPERELÍPTICAS

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

Curvas elípticas e hiperelípticas formam uma classe especial de curvas algébricas. Essas curvas são ferramentas importantes em várias áreas de aplicação, em especial na criptografia com chave pública. Emparelhamentos bilineares sobre curvas elípticas e hiperelípticas são funções matemáticas com propriedades de interesse para aplicações criptográficas. O algoritmo de criptografia de chave pública mais utilizado é o RSA. A criptografia sobre curvas elípticas e hiperelípticas (HECC) constitui uma alternativa ao RSA, já que os criptossistemas sobre tais curvas garantem um nível elevado de segurança, mesmo com chaves de tamanho bastante reduzido em relação às chaves RSA. Isso faz dos criptossistemas sobre curvas elípticas os mais propícios de ser implementados em ambientes computacionais restritos, ou seja, com baixo poder de processamento e memória reduzida, como smart cards, por exemplo. Neste trabalho, procurou-se compreender o funcionamento dos smart cards e também aprofundar o conhecimento sobre HECC por meio da implementação de programas baseados nessas tecnologias. As implementações mostraram que os criptossistemas implementados em smart cards são viáveis na prática, desde que os smart cards possuam co-processadores específicos para operações em curvas elípticas.

Criptografia - Curvas elípticas e hiperelípticas - Emparelhamentos bilineares