XII Congresso 22 a 24 de setembro de 2004
Interno de Iniciação Científica da UNICAMP
Ginásio Multidisciplinar da UNICAMP

E260

PARÂMETROS SEGUROS PARA CRIPTOGRAFIA DE CURVAS ELÍPTICAS SOBRE CORPOS FINITOS

Alberto Alexandre Assis Miranda (Bolsista PIBIC/CNPq) e Prof. Dr. Ricardo Dahab (Orientador), Instituto de Computação - IC, UNICAMP

A criptografia fornece segurança em comunicação pessoal, comércio eletrônico e validades de documentos digitais. Esta segurança está relacionada diretamente com o tempo mínimo necessário para se quebrar o sistema. Para que um criptossistema seja útil, deve-se estimar o tempo necessário para quebrá-lo com o melhor método disponível. No entanto, nem toda escolha de parâmetro tem dificuldade igual ao caso geral. Certos parâmetros permitem otimizações nos algoritmos de quebra diminuindo sensivelmente a segurança esperado do sistema. No caso particular de criptografia de curva elípticas, a segurança do sistemas será comprometida se a ordem da curva for igual a ordem do corpos sobre o qual ela está definida, se a ordem da curva somente tiver fatores pequenos ou se a primeira potência da ordem do corpo que iguala um módulo a ordem da curva for pequeno, ou ainda se o grau de extensão do corpo não for primo. Todos estes testes são triviais caso se tenha em mãos a ordem do corpo. Para tanto foi implementado o algoritmo de Schoof para contagem de pontos. Este algoritmo consiste em verificar a igualdade (p^n+1-t=ordem da curva) módulo vários primos, até que se defina o valor de t, o traço de Frobenius. A igualdade é verificada simbolicamente com as torsões e representações simbólicas do mapa de Frobenius e da multiplicação por escalar.

Criptografia - Curvas Elípticas - Algoritmo de Schoof