Aritmética de corpos finitos otimizada para criptografia de curvas elípticas

Orientado: Alberto Alexandre Assis Miranda
Orientador: Ricardo Dahab

Projeto de Iniciação Científica
Abril de 2002

Resumo

O objetivo deste projeto é a implementação de uma biblioteca de aritmética de precisão arbitrária para corpos finitos de ordem p^n, p primo, otimizada para operações de criptografia sobre curvas elípticas definidas sobre tais grupos.

1 Introdução

1.1 Motivação

A criptografia de chave pública tornou-se uma tecnologia imprescindível para provimento da maioria dos requisitos da segurança da informaçao em vários níveis da atividade humana moderna. Muitas dessas atividades utilizam redes de computadores abertas, desde as atividades do mercado financeiro, passando pelo comércio eletrônico, comunicação empresarial, segurança militar, até a simples comunicação pessoal. Os chamados criptossistemas de chave pública provêem cifragem dos dados, autenticacão de usuários e principalmente não-repúdio da autoria de documentos eletrônicos, pela utilização de assinaturas digitais.

Com o advento e disseminação dos computadores de bolso e outros dispositivos de comunicação portáteis, como telefones celulares, e sua utilização em comunicação pessoal e comércio eletrônico, tornou-se necessário otimizar as bibliotecas criptográficas dirigidas a esses aparelhos, que não possuem a mesma capacidade de processamento e armazenamento dos computadores pessoais de mesa. Uma das tecnologias criptográficas que têm se destacado nesse cenário é a baseada em curvas elípticas (ECC) definidas sobre corpos finitos. Em comparação com outras, já mais bem estabelecidas, como o conhecido sistema RSA, a de curvas elípticas possibilita o mesmo grau de segurança com chaves sensivelmente menores. Isso possibilita uma economia de espaço de memória e de tempo de processamento sem perda de segurança. O gráfico da Figura 1 [1] ilustra a relação dos tamanhos de chaves do RSA e de ECC para um mesmo nível de segurança.

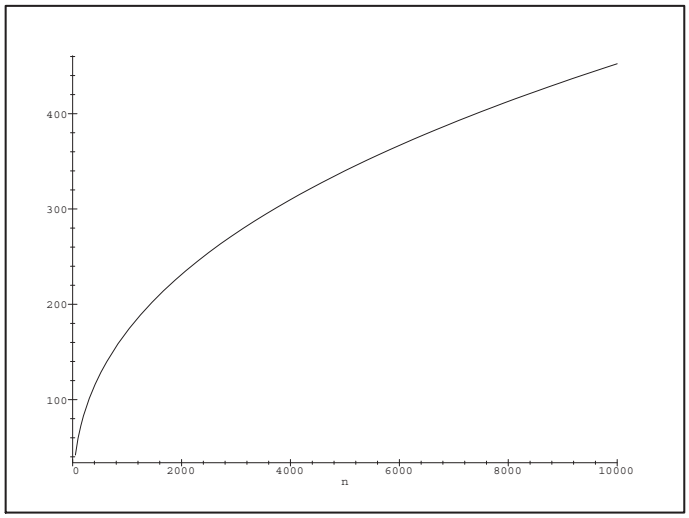

Figura 1: Comparação entre os tamanhos de chaves do RSA (eixo horizontal) e de curvas elípticas (eixo vertical)

1.2 Objetivos deste plano

Este projeto tem por objetivo criar uma biblioteca otimizada para operações de aritmética de corpos finitos dirigida à criptografia de curvas elípticas. Consequentemente, tanto a representação dos elementos dos corpos finitos quanto os algoritmos associados serão projetados para atender às particularidades das operações criptográficas de criptossistemas baseados em curvas elípticas. Essa decisão pode sacrificar a versatilidade e portabilidade da biblioteca mas, em vista do nosso objetivo maior de eficiência, este preço é aceitável. Esperamos, ao final do projeto, conseguir níveis de desempenho significantemente superiores aos das bibliotecas de propósito geral.

1.3 Organização deste documento

Na seção seguinte descrevemos os fundamentos matemáticos dos criptossistemas de curvas elípticas e as operações relevantes que queremos otimizar. A seguir, na Seção 3, fazemos um resumo das bibliotecas disponíveis atualmente. A Seção 4 contém uma descrição mais detalhada da extensão do projeto, suas fases e métodos de execução. Finalmente, na Seção 5, encontra-se o cronograma de atividades.

2 Criptografia de curvas elípticas

Uma curva elíptica é o conjunto de pontos que satisfazem uma equação do tipo $y^2 + axy + by = x^3 + cx^2 + dx + e$, onde a, b, c, d e e são elementos de um corpo. Os pontos da curva formam um grupo aditivo. A operação de soma nesse grupo tem uma interpretação geométrica: para P_1, P_2 dois pontos na curva, sua soma P_3 é a reflexão, com relação ao eixo de simetria da cúbica, do terceiro ponto da reta que contém P_1 e P_2

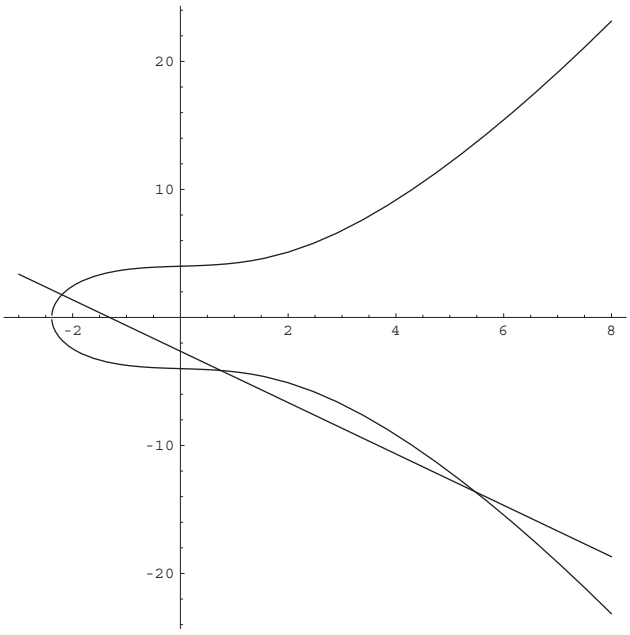

Figura 2: Definição de antisimétricos e da soma de dois pontos numa curva elíptica

como na Figura 2. Caso os pontos somados sejam iguais, a reta escolhida é a tangente. Já no caso da reta não interceptar novamente a cúbica (soma de antisimétricos) o resultado é a identidade aditiva. Define-se também a multiplicação de um ponto por um escalar (kP) como sendo $P + P + ... + P$ k vezes.

A criptografia por curvas elípticas se baseia na dificuldade de, dados P e kP, calcular k. Este é o chamado Problema do Logarítmo Discreto de Curvas Elípticas, para o qual até hoje não se conhece uma solução com complexidade de tempo subexponencial. Este fato torna possível o uso da operação das curvas elípticas como base de algoritmos criptográficos de chave pública. Mais especificamente, neste caso, P e kP compoem a chave pública e k é a chave privada.

Uma curva elíptica pode ser definida sobre qualquer corpo. Este projeto trabalha com os corpos de Galois de ordem p^n $(GF(p^n))$ com p primo maior que 2. Se $p = 3$ a equação da curva se simplifica para $y^2 = x^3 + ax^2 + bx + c$, já no caso de $p > 3$ a equação da curva se resume a $y^2 = x^3 + ax + b$. A soma de dois pontos é algebricamente definida pelas seguintes fórmulas [2].

Dados $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$, com $y_1 \neq -y_2$, defina

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{se } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{caso contrário.} \end{cases}$$

As coordenadas (x_3, y_3) do ponto $P_3 = P_1 + P_2$ são agora expressas como

$$x_3 = \lambda^2 - x_1 - x_2 \text{ e } y_3 = (x_1 - x_3)\lambda - y_1.$$

É evidente que a eficiência do cálculo da operação de soma de dois pontos da curva, e portanto do cálculo do produto escalar kP, dependem diretamente da eficiência com que as operações entre elementos do corpo são executadas. As operações que mais

consomem tempo são a multiplicação e a inversão (divisão). Assim, o desafio que nos propomos a enfrentar é o de otimizar essas operações tendo sempre em vista o seu impacto nas operações criptográficas.

3 Um breve resumo sobre bibliotecas existentes

As seguintes bibliotecas já foram examinadas com algum detalhe:

- **NTL:** biblioteca para manipulação de inteiros longos, vetores, matrizes, corpos finitos e polinômios sobre inteiros e sobre corpos finitos, implementada e mantida por Victor Shoup [4]. Está disponível para download gratuito na internet tem boa documentação, e tem uma interface bastante intuitiva em C++.
- **Lidia:** biblioteca para teoria dos números que implementa manipulações de várias estruturas matemáticas dentre elas $GF(p^n)$, desenvolvido pela Darmstadt University of Technology [3]. É gratuita para uso não comercial.

4 Detalhamento de objetivos e métodos

4.1 Objetivos

O projeto pretende implementar as operações básicas em corpos finitos utilizadas pela soma de pontos numa curva elíptica: soma, multiplicação, cálculo de inversos e de quadrados. Também devem ser implementadas operações de infra-estrutura de um corpo finito, tais como geração de polinômios irredutíveis e redução módulo tais polinômios. Num primeiro momento utilizaremos bibliotecas prontas para a aritmética de inteiros longos e para a aritmética com pontos da curva elíptica. Caso seja interessante durante o projeto, algumas bibliotecas inicialmente importadas serão desenvolvidas localmente.

4.2 Como

O projeto se organizará da seguinte forma:

Estudo. Nesta fase será feito o aprofundamento do estudo já realizado da literatura de algoritmos para arimética de corpos finitos.

Escolha dos algoritmos Será feita uma análise técnica da complexidade dos algoritmos estudados, buscando aqueles mais adequados ‘a implementação em dispositivos de recursos limitados.

Implementação Aqui os algoritmos escolhidos serão cuidadosamente implementados e eventuais erros de programação decorrentes disso eliminados.

Testes Com as implementações prontas, faremos então a análise do desempenho durante um uso normal do criptossistema alvo das funções criadas. Gera-se deste modo uma boa quantidade de dados que ajudará na fase de otimização. É feita também nesta fase a comparação dos tempos obtidos com os tempos de outras implementações disponíveis.

Otimização O principal objetivo do projeto: melhorar a eficiência das funções implementadas o máximo possível. Baseando-se nas informações obtidas na fase anterior, identificaremos quais funcionalidades do sistema deverão ser otimizadas. Experimentaremos várias mudanças possíveis no código em busca de melhorias específicas para curvas elípticas, tanto de implementação como possivelmente nos algoritmos.

Testes das modificações Com a biblioteca alterada, verificaremos a influência e utilidade das mudanças ocorridas, comparando-se novamente os tempos obtidos com os parâmetros já citados. Novas modificações serão feitas caso necessário.

Conclusões Finaliza-se o projeto com uma análise dos resultados obtidos, da satisfabilidade dos mesmos, e indicações de caminhos para outras pesquisas com o mesmo objetivo.

Disponibilização Após finalização total do projeto, o mesmo será disponibilizado para o público em geral.

4.2.1 Materiais e métodos

Para o desenvolvimento do projeto não são muitas as necessidades materiais. São necessários livros que estão disponíveis nas bibliotecas da Unicamp, laboratório de programação para implementação da biblioteca, já disponibilizado aos alunos dos cursos de computação pelo Instituto de Computação da Unicamp. Para os testes e comparações de desempenho se usará um computador AMD Athlon 1.2 GHz, 768 MB RAM, com o sistema Linux instalado.

5 Cronograma

FaseAgo	Set	Out	Nov	Dez	Jan	Fev	Mar	Abr	Mai	Jun	Jul	
Estudo	X	X	X									
Escolha dos algoritmos	X	X	X									
Implementação		X	X	X	X							
Testes					X	X						
Otimização							X	X	X	X	X	
Testes									X	X	X	X
Conclusões											X	X
Disponibilização												X

Referências

[1] Ian Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic Curves in Cryptography.* Number 265 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.

[2] Neal Koblitz. *A Course in Number Theory and Cryptography.* Springer-Verlag New York, Inc, 2 edition, 1987.

[3] LiDIA Group Darmstadt University of Technology. A c++ library for computational number theory. http://www.informatik.tu-darmstadt.de/TI/LiDIA/.

[4] Victor Shoup. Ntl: A library for doing number theory. http://shoup.net/ntl.