Métodos Gerais de Multiplicação por Escalar em Curvas Elípticas

Pedro Carlos da Silva Lara* **Fábio Borges de Oliveira**
Coordenação de Sistemas e Redes, CSR, LNCC,
25651–075, Petrópolis, RJ
E-mail: {pcslara,borges}@lncc.br

RESUMO

Em 1985, foi proposto, de forma independente, a aplicação de curvas elípticas em criptografia assimétrica [1]. A segurança deste método está baseada no Problema do Logaritmo Discreto (PLD), no entanto, diferentemente dos métodos anteriores, este usa como base o grupo formado pelos pontos de uma curva elíptica. Este criptossistema tem a vantagem de exigir uma chave de comprimento consideravelmente menor que a chave usada em alguns clássicos da criptografia assimétrica, tais como o RSA. Contudo, para criptografar dados, a operação mais importante e custosa é a multiplicação por escalar, que é equivalente a operação de exponenciação realizada quando se usa o PLD sobre grupos multiplicativos da forma $\mathbb{Z}_p$. Esta operação consiste em multiplicar um ponto P de uma curva elíptica Ω por um inteiro K, obtendo outro ponto, digamos $Q = KP$. Neste resumo iremos abordar brevemente algumas técnicas ultilizadas para a multiplicação por escalar em curvas elípticas gerais. Podemos falar basicamente de dois tipos de algoritmos: que usam o conceito de cadeias aditivas e que usam seqüências aditivas [2]. Na verdade uma cadeia aditiva para r é o conjunto $a_1 = 1, a_2, \ldots, a_n = r$ tal que para cada $i > 1$, existem $j, k \in (1 \leq j \leq k < i)$ tal que $a_i = a_j + a_k$. Uma cadeia aditiva é útil para acelerar a computação de g^r, sendo g um parâmetro fixo, e consequentemente poderá ser usado para acelerar o cálculo da multiplicação por escalar em curvas elípticas. Se $L(r)$ é o tamanho mínimo para uma cadeia aditiva então pode ser demonstrado que

$$L(r) = \log_2 r + (1 + o(1))\frac{\log_2 r}{\log_2 \log_2 r}$$

Na verdade, quanto menor a cadeia aditiva mais rápida é a computação de g^r. Quando precisamos elevar g a multiplas potências $(r_1, \ldots, r_n)$ usamos o conceito de seqüências aditivas. Uma seqüência aditiva para $r_1, \ldots, r_n$ é uma cadeia aditiva $a_1 = 1, \ldots, a_l$ que contenha $r_1, \ldots, r_n$. O comprimento mínimo para uma seqüência aditiva pode ser dada por

$$L(r_1, \ldots, r_n) = \log_2 r + (n + o(1))\frac{\log_2 r}{\log_2 \log_2 r}$$

onde $r = max(r_1, \ldots, r_n)$. Um artifício interessante na multiplicação por escalar em curvas elípticas é a ultilização de pré-computação para melhorar o desempenho. Na verdade, quando se é conhecido o ponto P *a priori* é bastante pertinente que se use uma técnica que ultiza pré-computação.

Referências

[1] Pedro C. S. Lara and Fábio Borges, *Curvas elípticas: Aplicação em criptografia assimétrica*, Workshop de Trabalhos de Iniciação Científica e de Graduação do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (Rio de Janeiro), 2007, pp. 1–10.

[2] A. M. Neto, *Multiplicação escalar eficiente em curvas elípticas*, Dissertação de Mestrado, IME – USP, 2006.

*Bolsista de iniciação científica PIBIC/CNPq