Curvas Elípticas de Aplicação Insegura

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

Em 1985, V. Miller [4] e N. Koblitz [2] propuseram independentemente a aplicação de curvas elípticas em criptografia de chave pública. A segurança deste método está baseada no Problema do Logaritmo Discreto (PLD). O PLD sobre curvas elípticas consiste em encontrar um inteiro k dado dois pontos de uma curva elíptica qualquer $P, Q \in \Omega$ onde $P = kQ$. A grande vantagem deste criptossistema é que exige uma chave de comprimento consideravelmente menor que a chave usada no RSA, ficando acessível a sistemas com restrições computacionais, tais como *smart cards*. Por exemplo, em curvas elípticas uma chave com 163 *bits* é equivalente a uma chave de 1024 *bits* no RSA. A redução do tamanho da chave é resultado de não existir um algoritmo de tempo sub-exponencial para resolver o PLD sobre curvas elípticas. O algoritmo mais rápido que se conhece possui tempo de execução puramente exponencial $O(\sqrt{n})$, em relação ao número de *bits* da ordem da curva [1], representada por n, no entanto, para resolver o PLD (no grupo multiplicativo $\mathbb{Z}_p^*$) e o Problema da Fatoração de Inteiros (PFI), que possuem complexidades equivalentes, existe um algoritmo de tempo sub-exponencial: $O(e^{(c+O(1))(\ln n)^{1/3}(\ln \ln n)^{2/3}})$, sendo c uma constante e $n = pq$. Neste resumo ressaltaremos a presença de dois tipos de curvas que apresentam certa "fraqueza" contra algoritmos específicos (algoritmos que trabalham com certos aspectos bem definidos para poder resolver o problema em questão), são elas: supersingulares (supersingular elliptic curve) e anômalas (anomalous elliptic curve). Pelo teorema de Hasse, sabemos que $\#\Omega(\mathbb{F}_q) = q+1-t$, onde $|t| \leq 2\sqrt{q}$, chamaremos t de traço de Frobenius. Uma curva elíptica é chamada de supersingular se, e somente se, $t \equiv 0 \mod p$. Seja $\Omega(\mathbb{F}_p)$ uma curva elíptica, definimos esta curva como anômala, se a ordem desta curva for p, ou seja, $\#\Omega = p$. Estas duas curvas devem ser evitadas, pois existem algoritmos eficientes contra ambas. Inicialmente, as curvas supersingulares foram consideradas promissoras para criptografia assimétrica, uma vez que permite uma velocidade maior na encriptação. Quando Ω está definida sobre o corpo $\mathbb{Z}_p$, com $p > 3$, pode-se demonstrar que Ω é supersingular se, e somente se, $t^2 \in \{0, p, 2p, 3p, 4p\}$, onde $\#\Omega = p + 1 - t$. Para o cálculo da ordem da curva, $\#\Omega$, existe um algoritmo bem eficiente que é devido a R. Schoof [5]; este algoritmo possui complexidade $O(\log^8 n)$. Em 1991, Menezes, Okamoto e Vanstone (MOV) [3] descobriram um algoritmo em tempo sub-exponencial para o cálculo de logaritmos discretos em curvas elípticas supersingulares. Este novo algoritmo possui complexidade equivalente ao PLD sobre grupos multiplicativos $\mathbb{Z}_p^*$, porém, como a chave criptográfica de algoritmos baseados em curvas elípticas é substancialmente reduzida, este algoritmo se torna bem eficiente. Na verdade, MOV usaram o emparelhamento Weil para reduzir o PLD sobre curvas elípticas para o PLD sobre grupos multiplicativos de corpos finitos $\mathbb{F}_q$ onde $q = p^m$. A eficiência do algoritmo de MOV está no fato que para o PLD sobre $\mathbb{F}_q$ existem algoritmos de tempo sub-exponencial. Um exemplo de curvas elípticas supersingulares sobre corpos da forma $\mathbb{F}_{2^m}$ é

*bolsista de Iniciação Científica PIBIC/CNPq

$y^2 + y = x^3 + ax + b$. Em 1991 A. Miyaji propôs o uso de curvas anômalas em criptografia, devido a algumas propriedades. Em 1999, Smart [6] descreveu métodos de ataques polinomiais em curvas elípticas anômalas (traço de Frobenius $t = 1$), dentre outros conceitos, este ataque usa o corpo dos números p-ádicos. Na verdade Smart mostrou que o isomorfismo de grupos

$$\psi : \Omega(\mathbb{F}_p) \to \mathbb{F}_p^+$$

pode ser eficazmente computado, sendo $\Omega(\mathbb{F}_p)$ uma curva anômala; logo calcular k tal que $P = kQ$ é equivalente a calcular k tal que $\psi(P) = k\psi(Q)$ onde $P, Q \in \Omega(\mathbb{F}_p)$. E conseqüentemente reduzindo o PLD em $\Omega(\mathbb{F}_p)$ para o PLD sobre grupos aditivos $\mathbb{F}_p^+$. Dados $a, b \in \mathbb{F}_p^+$ com $a \neq 0$ e p primo, o PLD em $\mathbb{F}_p^+$ (grupo aditivo dos restos módulo p) consiste em encontrar $l \in \{0, \ldots, p-1\}$ tal que $la \equiv b \pmod{p}$. Isto implica que $l \equiv ba^{-1} \pmod{p}$. Observe que isto pode ser facilmente resolvido através do algoritmo estendido de Euclides para encontrar a^{-1}. Com estas comprovações estas classes de curvas foram descontinuadas em protocolos de seguranças. Estes tipos de ataque não são viáveis nem estendíveis a outros tipos de curvas. É importante ressaltar que o número total de curvas supersingulares e curvas anômalas sobre um determinado corpo finito é demasiadamente menor do que o número total de curvas. No entanto é de extrema relevância que se leve em consideração as seguintes restrições: Seja $G = (x, y)$ um ponto base de uma curva elíptica $\Omega(\mathbb{F}_p) : y^2 = x^3 + ax + b$ e n a ordem do subgrupo $\langle G \rangle \subseteq \Omega(\mathbb{F}_p)$, $(\langle G \rangle = \{\alpha G : \alpha \in \mathbb{Z}\})$ considere $h = \frac{\#\Omega}{n}$.

i) $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$.
ii) $\#\Omega \neq p$.
iii) $t \not\equiv 0 \pmod{p}$.
iv) $h \leq 4$.

Sendo t o traço de Frobenius. A condição i) deve ser satisfeita para que o conjunto dos pontos da curva Ω venha a ser um grupo. A condição ii) exclui a presença de curvas anômalas. A restrição iii) é importante para detectarmos curvas elípticas supersingulares e finalmente a condição iv) determina se o ponto base G tem uma ordem segura, ou seja, dado um ponto $Q \in \Omega$, é intratável calcular k tal que $Q = kG$. Nos últimos tempos pesquisadores fizeram algumas contribuições em algoritmos já existentes para o cálculo de logaritmos discretos sobre curvas elípticas, porém, se as restrições para a segurança forem alcançadas não existe algoritmo eficiente para o PLD sobre curvas elípticas.

Referências

[1] Daniel M. Gordon and Kevin S. McCurley, *Massively parallel computation of discrete logarithms*, Lecture Notes in Computer Science **740** (1993), 312–323.

[2] Neal Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation **48** (1987), no. 177, 203–209.

[3] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto, *Reducing elliptic curve logarithms to logarithms in a finite field*, STOC '91: Proceedings of the twenty-third annual ACM symposium on Theory of computing (New York, NY, USA), ACM Press, 1991, pp. 80–89.

[4] Victor S. Miller, *Use of elliptic curves in cryptography*, Advances in cryptology—CRYPTO '85 (Santa Barbara, Calif., 1985), Lecture Notes in Comput. Sci., vol. 218, Springer, Berlin, 1986, pp. 417–426. MR MR851432 (88b:68040)

[5] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Th'eor. Nombres Bordeaux (1995), 219–254.

[6] N. P. Smart, *The discrete logarithm problem on elliptic curves of trace one*, Journal of Cryptology: the journal of the International Association for Cryptologic Research **12** (1999), no. 3, 193–196.