Avaliação de Segurança em Curvas Elípticas Usando o Corpo dos Números p-ádicos

Marcio Prudêncio Belleza[1]
Fábio Borges[1]

[1] Laboratório Nacional de Computação Científica (LNCC)
25651-075, Petrópolis - RJ - Brasil

{mbelleza,borges}@lncc.br

Abstract. *In 1999, N. P. Smart provided a very efficient algorithm for solving the elliptic curve discrete logarithm problem over a prime finite field $\mathbb{F}_p$, where p is prime, in linear time when the elliptic curve $E(\mathbb{F}_p)$ is anomalous, i.e., $\#E(\mathbb{F}_p) = p$. In this paper, we show two security requirements in cryptography and focus on anomalous elliptic curve using p-adic numbers.*

Resumo. *Em 1999, N. P. Smart propôs um algoritmo muito eficiente para resolver o problema do logaritmo discreto em curvas elípticas sobre um corpo finito $\mathbb{F}_p$, onde p primo, em tempo linear quando a curva elíptica $E(\mathbb{F}_p)$ é anômala, i.e., $\#E(\mathbb{F}_p) = p$. Neste trabalho, apresentamos dois requisitos de segurança em criptografia e focamos nas curvas elípticas anômalas usando os números p-ádicos.*

1. Introdução

A partir de meados da década de 80, [Koblitz 1987] e [Miller 1986] apresentaram, independentemente, o uso de curvas elípticas em criptografia de chave pública. Os métodos propostos baseiam-se no clássico Problema do Logaritmo Discreto (PLD - *Discrete Logarithm Problem*). A segurança de usarmos o PLD baseado em curvas elípticas na criptografia é garantida porque os melhores algoritmos para solucioná-lo têm complexidade exponencial. De fato, não existir um algoritmo do tipo subexponencial para resolver tal problema garante uma chave de comprimento bem menor que o da chave usada no RSA, introduzido por [Rivest et al. 1978]. Porém, para escolher curvas elípticas em criptografia é necessário eliminar dois tipos de curvas, são elas: supersingulares (traço de Frobenius igual a zero) e anômalas (traço de Frobenius igual a um). O PLD sobre estas curvas é reduzido a um problema que pode ser resolvido por algoritmos específicos. [Borges de Oliveira 2017] apresenta um resumo de requisitos de segurança para curvas elípticas. [Menezes et al. 1993] apresentaram um algoritmo com complexidade subexponencial para resolver o PLD sobre curvas supersingulares e [Smart 1999] apresentou um algoritmo com complexidade linear para resolver o PLD sobre curvas anômalas. [Menezes et al. 1993] reduziram o PLD sobre curvas elípticas supersingulares a um PLD em um corpo finito. [Smart 1999] atacou o problema usando números p-ádicos, com destaque para a aplicação de um resultado muito importante no estudo destes números, conhecido como Lema de Hensel.

O estudo de números p-ádicos é mais recente do que o de curvas elípticas e foi introduzido por Kurt Hensel (1861-1941). Segundo [Koblitz 1977], o Lema de Hensel é

frequentemente chamado de Método de Newton p-ádico porque a técnica de aproximação usada é essencialmente a mesma que o Método de Newton para encontrar a raiz de uma equação polinomial com coeficientes reais. [Koblitz 1977] afirmou que este lema é muito melhor que o Método de Newton: no caso p-ádico, é garantida a convergência para uma raiz do polinômio; no caso real, o Método de Newton nem sempre converge.

[Dragovich et al. 2017] mostraram que os números p-ádicos são aplicados em diversas ciências. Estes números foram relevantes na prova do Último Teorema de Fermat, veja [Wiles 1995]. Atualmente, eles foram usados em uma descoberta que garantiu a medalha Fields para o matemático alemão Peter Scholze, com o tema "Mapas de período na geometria p-ádica".

Nós, assim como [Smart 1999], acreditamos na eficiência da teoria de números p-ádicos no desenvolvimento de novos métodos na avaliação de segurança em curvas elípticas. Na Seção 2, apresentamos os conceitos básicos dos números p-ádicos. Na Seção 3, apresentamos como avaliamos curvas elípticas com p-ádicos e fornecemos um legível exemplo numérico. Na Seção 4, apresentamos as conclusões.

2. Conceitos Básicos de Números p-ádicos

Qualquer $x \in \mathbb{Z}$, $x \neq 0$, pode ser escrito como $x = p^v x'$, onde p é um primo e p não divide x'. Dessa forma, a valuação de x é definida por $v_p(x) = v$. Se $y \in \mathbb{Q}$, com $y = \frac{a}{b}$, então $v_p(y) = v_p(a) - v_p(b)$. Assim, a norma de y é definida por $|y|_p = p^{-v}$, com $y \neq 0$. Esta norma define uma métrica $|y - w|_p$ sobre $\mathbb{Q}$, e satisfaz a desigualdade triangular forte, i.e., $|y + w|_p \leqslant \max\{|y|_p, |w|_p\}$. Esta norma é não-arquimediana provendo uma geometria totalmente diferente do que seria intuitivo, e.g., onde todo triângulo é isósceles e todo ponto de um círculo é o centro deste círculo.

O corpo dos números p-ádicos $\mathbb{Q}_p$ é o completamento de $\mathbb{Q}$ ($\mathbb{Q} \subset \mathbb{Q}_p$) relativamente à norma $|.|_p$. Então, o anel dos inteiros p-ádicos é definido por

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\}.$$

Os números p-ádicos são escritos de forma única

$$\sum_{i \geqslant -n} a_i p^i = a_{-n}p^{-n} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots, \text{ com } a_i \in \{0, \ldots, p-1\}. \quad (1)$$

Como já afirmamos, o Lema de Hensel é um resultado muito importante em diversas áreas. Ele afirma que dada uma função $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ com coeficientes inteiros p-ádicos, dada $f'(x) = c_1 + 2c_2 x + \cdots + n c_n x^{n-1}$ a derivada de f, e dado a_0 um inteiro p-ádico tal que $f(a_0) \equiv 0 \mod p$ e $f'(a_0) \not\equiv 0 \mod p$, então existe um único inteiro p-ádico a tal que $f(a) = 0$ e $a \equiv a_0 \mod p$.

Como exemplo, temos que $\sqrt{2} \in \mathbb{Q}_7$, logo

$$f(x) = x^2 - 2 \Rightarrow f'(x) = 2x.$$

Se considerarmos $a_0 \in \{0, \cdots, 6\}$, então as condições do lema são satisfeitas somente para $a_0 = 3$ e $a_0 = 4$. Logo, o lema garante a existência de duas raízes distintas para f. Usando SAGE, encontramos as raízes 7-ádicas de f conforme (1), elas são dadas por

$$3 + 1.7 + 2.7^2 + 6.7^3 + 1.7^4 + O(7^5)$$

e

$$4 + 5.7 + 4.7^2 + 5.7^4 + O(7^5),$$

que correspondem, respectivamente, às raízes $\sqrt{2}$ e $-\sqrt{2}$. Note que também poderíamos ter raízes complexas representadas por números p-ádicos. Especificamente, temos um resultado importante sobre raízes de polinômios que garante que $x^2 = -1$ tem solução em $\mathbb{Q}_p$ se e somente se $p \equiv 1 \mod 4$.

Para maiores detalhes sobre números p-ádicos, consulte [Koblitz 1977] e [Gouvêa 1997].

3. Avaliação Usando Números p-ádicos

O algoritmo proposto por [Smart 1999] pode ser descrito da seguinte forma:

Seja $\overline{E}(\mathbb{F}_p)$ uma curva elíptica de traço um sobre um corpo finito $\mathbb{F}_p$ com p primo.

Dados dois pontos $\overline{P}, \overline{Q} \in \overline{E}(\mathbb{F}_p)$, o PLD a ser resolvido significa determinar m tal que

$$\overline{Q} = [m]\overline{P} \tag{2}$$

Primeiramente, aplica-se um "lift" dos pontos $\overline{P}$ e $\overline{Q}$ para os pontos $P, Q \in E(\mathbb{Q}_p)$. Para isso, escreve-se $\overline{P} = (a, b)$ e $P = (x, y)$, onde $x = a$ e y é determinado aplicando o Lema de Hensel com $a_0 = b$. Este mesmo procedimento é realizado para o ponto Q. Em seguida, calcula-se $[p]P$ e $[p]Q$. Aplicando o logaritmo elíptico p-ádico ψ_p nos termos $[p]P$ e $[p]Q$, temos que m é determinado pela fórmula

$$m \equiv \frac{\psi_p([p]Q)}{\psi_p([p]P)} \mod p$$

onde

$$\psi_p((x, y)) \equiv \frac{-x}{y} \mod p^2.$$

Para mais detalhes, ver [Smart 1999] e [Silverman 2009].

Para ilustrar o algoritmo, vejamos um exemplo numérico onde $\overline{E}$ é uma curva elíptica sobre um corpo finito pequeno $\mathbb{F}_7$, definida por $y^2 = x^3 + 6x + 5$. O grupo $\overline{E}(\mathbb{F}_7)$ tem 7 elementos, logo ela é anômala. Sobre esta curva, pretende-se resolver o PLD dado por (2), onde $\overline{Q} = (2, 5)$ e $\overline{P} = (2, 2)$, ou seja,

$$(2, 5) = m(2, 2).$$

Os pontos $P, Q \in E(\mathbb{Q}_7)$ que foram obtidos a partir do "lift" nos pontos $\overline{P}$ e $\overline{Q}$ com aplicação do Lema de Hensel são dados por

$$P = (2, 2 + 6.7 + O(7^2))$$

e

$$Q = (2, 5 + 0.7 + O(7^2)).$$

Então, calcula-se $[7]P$ e $[7]Q$, obtendo

$$[7]P = (2.7^{-2} + O(7^{-1}), 1.7^{-3} + O(7^{-2}))$$

e

$$[7]Q = (2.7^{-2} + O(7^{-1}), 6.7^{-3} + O(7^{-2})).$$

O logaritmo elíptico 7-ádico nos termos anteriores resulta em

$$\psi_7([7]Q) = 2.7 + O(7^2)$$

e

$$\psi_7([7]P) = 5.7 + O(7^2).$$

Portanto,

$$m = \frac{\psi_7([7]Q)}{\psi_7([7]P)} = 6 + O(7).$$

O resultado $m = 6$ pode ser facilmente verificado como solução correta. Os elementos do grupo formado pela curva elíptica são dados por

$$\overline{E} = \{\infty, (2,2), (4,3), (3,1), (3,6), (4,4), (2,5)\}.$$

A Figura 1 mostra os pontos ordenados pelo gerador $(2,2)$ do grupo cíclico da curva elíptica anômala, destacando uma simetria com a reta em vermelho.

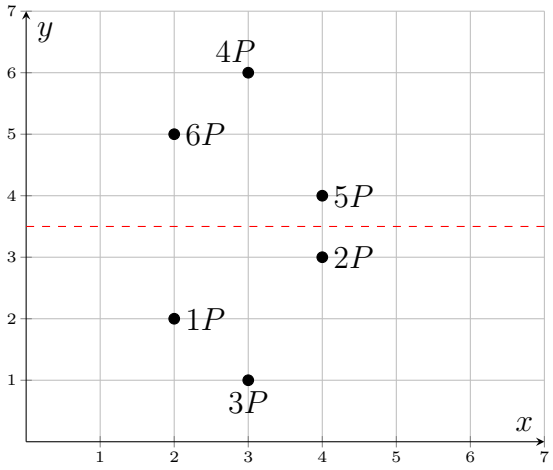

Figura 1. Pontos ordenados da curva elíptica anômala $y^2 = x^3 + 6x + 5$.

4. Conclusão

Mostramos que evitar curvas elípticas anômalas e supersingulares é um requisito de segurança e que se faz necessário avaliar as curvas escolhidas para evitar curvas que possam ser quebradas. Inclusive, fornecemos um exemplo numérico de como quebrar o PLD. Por se tratar de um trabalho em andamento, mostramos apenas os detalhes das curvas elípticas anômalas que são atacadas com um algoritmo linear. Por esse motivo, não são seguras em criptografia. Porém, no estudo de criptografia pós-quântica as curvas elípticas supersingulares tornam-se seguras com o uso de isogenias. Em trabalhos futuros, pretendemos aplicar os números p-ádicos tanto para atacar quanto para assegurar padrões de segurança em algoritmos criptográficos baseados em curvas elípticas.

Agradecimentos

Gostaríamos de agradecer ao Pronametro e a FAPERJ pelo apoio no desenvolvimento deste trabalho.

Referências

Borges de Oliveira, F. (2017). *Selected Privacy-Preserving Protocols*, pages 61–100. Springer International Publishing, Cham.

Dragovich, B., Khrennikov, A. Y., Kozyrev, S. V., Volovich, I. V., and Zelenov, E. I. (2017). p-adic mathematical physics: the first 30 years. *p-Adic Numbers, Ultrametric Analysis and Applications*, 9(2):87–121.

Gouvêa, F. Q. (1997). *p-adic Numbers*, pages 43–85. Springer Berlin Heidelberg, Berlin, Heidelberg.

Koblitz, N. (1977). *p-adic numbers*, pages 1–20. Springer US, New York, NY.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209.

Menezes, A. J., Okamoto, T., and Vanstone, S. A. (1993). Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646.

Miller, V. S. (1986). Use of elliptic curves in cryptography. In *LNCS 218 on Advances in Cryptology—CRYPTO 85*, pages 417–426, New York, NY, USA. Springer-Verlag New York, Inc.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126.

Silverman, J. H. (2009). *Elliptic Curves over Finite Fields*, pages 137–156. Springer New York, New York, NY.

Smart, N. P. (1999). The discrete logarithm problem on elliptic curves of trace one. *Journal of Cryptology*, 12(3):193–196.

Wiles, A. J. (1995). Modular elliptic curves and fermat's last theorem. *ANNALS OF MATH*, 141:141.