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

Marcio Belleza
Fábio Borges

Laboratório Nacional de Computação Científica - LNCC

10 de dezembro de 2018

Organização do Trabalho

- Introdução
- Conceitos Básicos de Números p-ádicos
- Avaliação Usando Números p-ádicos
- Conclusões
- Referências

Introdução

- [Koblitz 1987] e [Miller 1986] apresentaram, independentemente, o uso de curvas elípticas em criptografia de chave pública, ambos baseados no clássico PLD.
- A segurança de usarmos o PLD baseado em curvas elípticas na criptografia é garantida porque os melhores algoritmos para solucioná-lo têm complexidade exponencial.
- Para escolher curvas elípticas em criptografia é necessário eliminar dois tipos de curvas, são elas: supersingulares e anômalas.

Introdução

- [Menezes et al. 1993] apresentaram um algoritmo com complexidade subexponencial para resolver o PLD sobre curvas supersingulares.

- [Smart 1999] apresentou um algoritmo com complexidade linear para resolver o PLD sobre curvas anômalas.

- [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.

Conceitos Básicos de Números p-ádicos

- 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.
- [Dragovich et al. 2017] mostraram que os números p-ádicos são aplicados em diversas ciências. [Wiles 1995] aplicou estes números na prova do Último Teorema de Fermat.
- Em 1923, Hasse demonstrou o potencial dos números p-ádicos ao formular o princípio local-global: uma equação tem uma solução em $\mathbb{Q}$ se e somente se tem uma solução em $\mathbb{Q}_p$ para cada primo p.

Conceitos Básicos de Números p-ádicos

Sejam $x, y \in \mathbb{Q}$, a norma de x é definida por $|x|_p = p^{-v}$, com $x \neq 0$. Esta norma define uma métrica $|x - y|_p$ sobre $\mathbb{Q}$, e satisfaz a desigualdade triangular forte, i.e., $|x + y|_p \leqslant \max\{|x|_p, |y|_p\}$.

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

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

Conceitos Básicos de Números p-ádicos

O Lema de Hensel afirma que dada uma função f definida por $f(x) = c_0 + c_1x + \cdots + c_nx^n$ com coeficientes inteiros p-ádicos, dada $f'(x) = c_1 + 2c_2x + \cdots + nc_nx^{n-1}$ a sua derivada, 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

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

Conceitos Básicos de Números p-ádicos

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, 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 $-\sqrt{2}$.

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 $P, Q \in E(\mathbb{Q}_p)$.

Avaliação Usando Números p-ádicos

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 $a_0 = b$. 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].

Avaliação Usando Números p-ádicos

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, 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

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

Avaliação Usando Números p-ádicos

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,

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

Conclusões

- Mostramos que evitar curvas elípticas anômalas e supersingulares é um requisito de segurança.
- Por se tratar de um trabalho em andamento, apresentamos apenas os detalhes das curvas elípticas anômalas que são atacadas com um algoritmo linear.
- 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.

Referências I


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.


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.

Referências II


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.


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.

Referências III

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