Uma Introdução a Criptografia de Curvas Elípticas

Prof Antônio

Universidade Federal do Maranhão

antonio.batista@ufma.br

8 de Março de 2016

Sumário

Definição

Seja F um corpo, e, a, b sejam escalares em F tal que a cúbica $X^3 + aX + b$ não tenha raízes repitidas. Uma curva elíptica E definida sobre um corpo F é o conjunto de soluções $(x, y) \in F^2$ para a equação $Y^2 = X^3 + aX + b$ mais um ponto no infinito denotado por *infinity*.

- são baseados no Problema do Logarítmo Discreto em Curvas Elípticas.
- Definido por Koblitz como **Dada uma Curva E definida sobre $GF(q)$ e dois pontos $P, Q \in E$, encontrar um inteiro x tal que $Q = xP$ se tal x existe**.
- Exemplo: Considere a Curva Elíptica E dada pela equação $Y^2 = X^3 + X - 1 \ mod \ 7$:

Exemplo

São todos os pontos sobre a curva $Y^2 = X^3 + X - 1 \ mod\ 7$

1. Seja $P(1,6)$ e $G(1,1)$ encontrar um x tal que $xP = G$.
2. $10P = (P + P + P + P + P + P + P + P + P + P)$
3. A ordem do ponto P é 11

Pontos	$K * P$
(1,6)	P
(2,3)	2P
(6,2)	3P
(4,2)	4P
(3,6)	5P
(3,1)	6P
(4,5)	7P
(6,5)	8P
(2,4)	9P
(1,1)	10P
infinity	11P

Elliptic Curve Group Law

- Dado $P_1, P_2 \in E(K)$, K um corpo, esse algoritmo computa um terceiro ponto $R = P_1 + P_2 \in E(K)$.

1. If $P_1 = \infty$ set $R = P_2$ or if $P_2 = \infty$ set $R = P_1$ and terminate. Otherwise write $(x_i, y_i) = P_i$.
2. If $x_1 = x_2$ and $y_1 = -y_2$, set $R = \infty$ and terminate.
3. Set $\lambda = \begin{cases} (3{x_1}^2 + a)/(2y_1), & \text{if} \quad P_1 = P_2, \\ (y_1 - y_2)/(x_1 - x_2), & \textit{otherwise}. \end{cases}$
4. Then $R = (\lambda^2 - x_1 - x_2 \ , -\lambda x_3 - v)$, where $v = y_1 - \lambda x_1$ and $x_3 = \lambda^2 - x_1 - x_2$ is the x-coordinate of R.

Método Binário - Multiplicação escalar

Algorithm 1 Método Binário

Entrada: Representação Binária de k e um ponto P

Saída: $Q = kP$

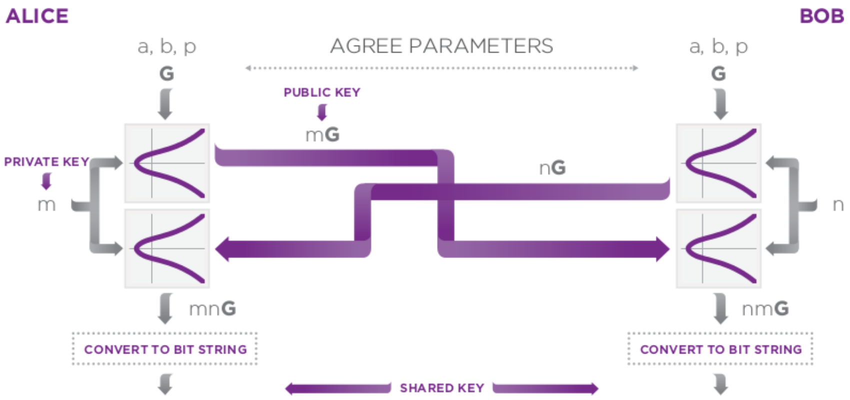
```
Q = P
for i = n − 2 to 0 do
    Q = 2Q {Doubling}
    if k_i = 1 then
        Q = Q + P {Addition}
    end if
end for
return Q
```

Método Binário - Multiplicação escalar

- Exemplo: calcular 19P.

$k_4 2^4 +$	$k_3 2^3 +$	$k_2 2^2 +$	$k_1 2^1 +$	$k_0 2^0 =$	19
k4	k3	k2	k1	k0	
1	0	0	1	1	
	2P	4P	8P+P	18P+P	

ECDH



ALICE
BOB
a, b, p
G
AGREE PARAMETERS
a, b, p
G
PUBLIC KEY
mG
PRIVATE KEY
m
nG
n
mnG
nmG
CONVERT TO BIT STRING
CONVERT TO BIT STRING
SHARED KEY

Criptossistema de Curvas Elípticas Elgamal

- *Alice* quer enviar uma mensagem m criptografada para *Bob*. Para tornar simples o nosso entendimento vamos supor que $m(2,4)$ é um ponto da Curva.

- São publicamente conhecidos a curva $Y^2 = X^3 + X - 1 \; mod \; 7$ e o ponto da curva $P(1,6)$ usados por Alice e Bob.

- primeiramente, Bob escolhe um $a = 63$ inteiro aleatório o qual ele mantém em segredo; e em seguida, computa a sua chave pública $\beta = aP$ e a publica.

- $\beta = 63P = (6,5)$

Criptossistema de Curvas Elípticas Elgamal

- Para transmitir uma mensagem m cifrada para *Bob*, Alice :
- escolhe um $k = 7$ inteiro aleatório e computa os pontos $y_1 = kP$ e $y_2 = m + k\beta$;
  - $y_1 = 7P = (4, 5)$
  - $y_2 = m + k\beta = (2, 4) + (1, 6) = (1, 1)$
- por fim, ela envia o par de pontos (y_1, y_2).

- Para ler a mensagem *Bob*::

- multiplica o primeiro ponto do par de pontos por sua secreta a (ay_1);
  - $ay_1 = 63(4,5) = (1,6)$
- e em seguida, subtrai o resultado do segundo ponto no par de pontos $(m = y_2 - ay_1)$.
  - $m = (1,1) - (1,6) = (2,4)$

Qebrando o Criptossistema de Curvas Elípticas Elgamal

- Eva a intrusa conhece:
  - a curva usada $Y^2 = X^3 + X - 1 \; mod \; 7$;
  - o ponto $P(1,6)$ escolhido por Alice e Bob;
  - o par de pontos (y_1, y_2) $((4,5),(1,1))$interceptado;
  - a chave pública de Bob $\beta(6,5)$;
- Eva precisa resolver o Problema do Logarítmo Discreto em Curvas Elípticas:
  - encontrar o inteiro k escolhido por Alice tal que $y_1 = kP$, ou seja, (4,5) $=$ k(1,6).

Baby Step Giant Step for ECDLP

Algorithm 2 Baby Step Giant Step for ECDLP

In: an point generator G of order N and $P = nG$

Out: n

$m \leftarrow \lceil \sqrt{N} \rceil$
for $j \leftarrow 0$ to $m - 1$ **do**
    Compute jP and store (j,jP)
end for
for $i \leftarrow 0$ to $m - 1$ **do**
    Compute G − imP
    if $G - imP = jP$ for some j **then**
        return $n = j + im$
    end if
end for

MAPPING MESSAGES into POINTS of ELLIPTIC CURVES (Koblitz's Method)

- Seja K um inteiro grande tal que uma taxa de falha de $\frac{1}{2^k}$ seje aceitável quando tentando codificar uma mensagem em um ponto.
- Para $j \in \{0, 1, 2, ..., k-1\}$ verifique se para $x = mK + j$, $x^3 + ax + b \ (mod \ p)$ é um quadrado (square) de um inteiro y, ou seja, $y^2 \equiv x^3 + ax + b \ (mod \ p)$.
- Se um tal j for encontrado, a codificação é feita, Se não o algoritmo falha (com probabilidade $\frac{1}{2^k}$ porque $x^3 + ax + b \ (mod \ p)$ é um quadrado aproximadamente metade das vezes).
- A fim de recuperar a mensagem m a partir do ponto (x, y), nós computamos: $\lfloor \frac{x}{k} \rfloor$

MAPPING MESSAGES into POINTS of ELLIPTIC CURVES(example)

- Vamos dizer que nosso alfabeto consiste das letras $A, B, C, ..., X, Y, Z$ codificados como $10, 11, 12, ..., 33, 34, 35$.

- Agora vamos converter a letra B em um ponto da curva $Y^2 = X^3 - X + 188 \ mod \ 751$, ou seja, $m = 11$.

MAPPING MESSAGES into POINTS of ELLIPTIC CURVES(example)

$$Y^2 = X^3 - X + 188 \ mod \ 751$$

k=11

m=11

j	x = mK + j	**(x,y)**	add bits
0	121		1111001
1	122		1111010
2	123		1111011
3	124	(124,354)	1111100
4	125	(126,275)	1111101
5	126		1111110
6	127		1111111
7	128	(128,252)	10000000
8	129		10000001
9	130		10000010
10	131		10000011

pare.

MAPPING MESSAGES into POINTS of ELLIPTIC CURVES(example)

- $a = 317689081251325503476317476413827693272746955927$,
  $b = 790528966078787587181205720257185354321006519 34$ e
  $p = 785963102379428822376694789446897396207498568951$
- Agora vamos converter os números a seguir em pontos da curva $Y^2 = X^3 + aX + b \ mod \ p$:
- IN GALOIS FIELDS, FULL OF FLOWERS, PRIMITIVE ELEMENTS DANCE FOR HOURS.

1924411711222519294 1
16191522142944 11631
2222412516411622253 3
1528294441262819231 9
3019321541152215231 5
2430294114112413154 1
1625284118253128294 3

Aspectos de Segurança

- Por quê os parâmetros para curvas elípticas (160-256 bit) são significativamente menores do que para RSA (1024-3072 bit)?
  - ataques sobre grupos de curvas elípticas são mais fracos do que os algoritmos de fatoração ou ataques para encontrar o Logarítmo discreto sobre inteiros.
  - os melhores ataques conhecidos sobre curvas elípitcas são os métodos do Baby-Step Giant-Step and Pollard-Rho.
  - a compexidade desses métodos: em média, são requeridos $\sqrt{p}$ passos antes do problema ECDLP poder ser resolvido.