Bernd Borchert

Univ. Tübingen WS 13/14

Vorlesung

Kryptographie

Teil 9
(Prof. Reinhardt)

Elliptische Kurven

24.1.14

Diskreter Logarithmus:

Gesucht $0 \le a \le p-2$ mit $\alpha^a \equiv \beta \bmod p$

Gegeben: p prim, $\alpha \in \mathbb{Z}_p^*$ erzeugend, $\beta \in \mathbb{Z}_p^*$

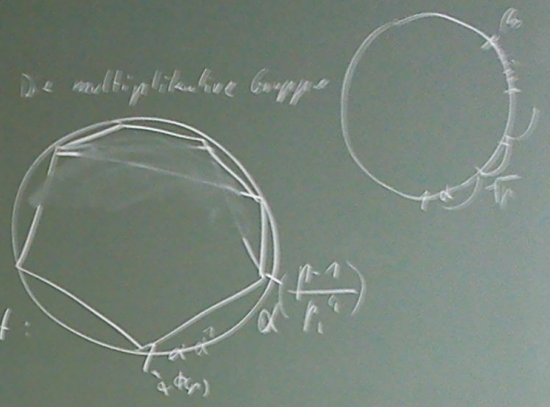
Pohlig-Hellman Algorithmus

Sei $p-1 = \prod_{i=1}^{k} p_i^{c_i}$

$\mathbb{Z}_p^*$ ist Kreuzprodukt von Gruppen der Größe $p_i^{c_i}$

Idee: Berechne den Exponenten a modulo jeden $p_i^{c_i}$ danach Zusammensetzen nach dem Chinesischen Restklassensatz

Die multiplikative Gruppe



Die Berechnung von $\log_\alpha \beta \bmod q^c$ geht wie folgt:

$\gamma_i = \alpha^{(p-1)i/q} \bmod p$ für $0 \le i \le q-1$

$\beta_0 = \beta$, For $j := 0$ to $c-1$ do begin

$\delta := \beta^{(p-1)/q^{j+1}}$, finde i mit $\delta = \gamma_i$; $a_j = i$; $\beta_{j+1} = \beta_j \alpha^{-a_j q^j}$

end

$\log_\alpha \beta \bmod q^c = \sum_{i=0}^{c-1} a_i q^i$

Bsp.: $p = 29$ $p-1 = 28 = 2^2 \cdot 7^1$ $\alpha = 2$ $\beta = 18$

$q = 2$ $c = 2$ $\gamma_0 = 1$ $\gamma_1 = \alpha^{28/2} \bmod 29 = 28$

$\delta = \beta^{28/2} \bmod 29 = 28 \Rightarrow a_0 = 1$

$\beta_1 = \beta_0 \alpha^{-1} \bmod 29 = 9$ $\delta = \beta_1^{28/4} \bmod 29 = 9^2 \bmod 29 = 28 \Rightarrow a_1 = 1$

$(\log_2 18) \bmod 4 = 3$

$q = 7$ $c = 1$ $\delta = \beta^{28/7} \bmod 29 = 18^4 \bmod 29 = 25$

$\gamma_1 = \alpha^{28/7} \bmod 29 = 16$, $\gamma_2 = \alpha^{28 \cdot 2/7} \bmod 29 = 24$, $\gamma_3 = \alpha^{28 \cdot 3/7} \bmod 29 = 7$, $\gamma_4 = 25$

$(\log_2 18) \bmod 7 = 4$

$a \equiv 3 \bmod 4$, $a \equiv 4 \bmod 7$ } mit Ch. Restkl.s. $a \equiv 11 \bmod 28$ zur Probe $2^{11} \bmod 29 = 18$

Laufzeit ist durch die größte der Primzahlen p_i in der Faktorisierung von $p-1$ bestimmt; das lässt sich durch Kombination mit Pollards ρ-Algorithmus auf $O(\sqrt{p_i})$ reduzieren

Ist $p-1 = 2^s \cdot t^{\text{ungerade}}$ so sind die s niederwertigsten Bits von $\log_\alpha \beta$ effizient zu berechnen, der Rest aber so schwer wie $\log_\alpha \beta$ selbst.

Bsp. $p \equiv 3 \pmod 4 \Rightarrow s = 1$ d.h. das niederwertigste Bit kann berechnet werden aber angenommen es gibt einen Algorithmus $L_2(\beta)$ der das 2-niederwertige Bit berechnen kann, so kann folgender Algorithmus $\log_\alpha \beta$ berechnen:

x_0 = niederwertigstes Bit von $\log_\alpha \beta$; $\beta := \beta / \alpha^{x_0} \bmod p$, $i := 1$

while $\beta \neq 1$ do

$x_i = L_2(\beta)$, $\gamma = \beta^{(p+1)/4} \bmod p$

if niederwertigstes Bit von $\log_\alpha \beta = x_i$ then $\beta = \gamma$ else $\beta = p - \gamma$

$\beta = \beta / \alpha^{x_i} \bmod p$; $i := i+1$

$$\log_\alpha \beta = \sum_{i \geq 0} x_i 2^i$$

Index Calculus Methode

Idee: Wähle Faktorbasis $B = \{p_1 \dots p_B\}$

Konstruiere $\approx B + 10$ Kongruenzen mod p der Form

$$\alpha^{x_j} \equiv p_1^{a_{1j}} p_2^{a_{2j}} \dots p_B^{a_{Bj}} \pmod p$$

$$x_j \equiv a_{1j} \log_\alpha p_1 + \dots a_{Bj} \log_\alpha p_B \pmod{p-1}$$

Mit linearer Algebra können die $\log_\alpha p_i$ mit $i \leq B$ berechnet werden.

Für gegebenes β wähle zufälliges $s \leq p-2$ und versuche $\gamma = \beta \alpha^s \bmod p$ über der Faktorbasis zu faktorisieren.

$$\beta \alpha^s \equiv p_1^{c_1} p_2^{c_2} \dots p_B^{c_B} \pmod p$$

$$\log_\alpha \beta + s \equiv c_1 \log_\alpha p_1 + \dots c_B \log_\alpha p_B \pmod{p-1}$$

Bsp.: $p = 10007$, $\alpha = 5$, $B = \{2, 3, 5, 7\}$, "glückliche" Exponenten $4063, 5136, 9865$

$5^{4063} \bmod 10007 = 2 \cdot 3 \cdot 7$; $\log_5 2 + \log_5 3 + \log_5 7 = 4063 \pmod{10006}$

$\log_5 2 = 6578$, $\log_5 3 = 6190$, $\log_5 7 = 1301$

$\beta = 9451$

$s = 7736$

$\gamma = 8400 = 2^4 3^1 5^2 7^1$

$\log_5 \beta = 4 \log_5 2 + 2 \log_5 5 + \dots$

$= 6057$

Diskreten Logarithmus in $(G, \circ)$: Gegeben: G Gruppe mit Verknüpfung $\circ$

$\alpha \in G$, $\beta \in H = \{\alpha^i \mid i \geq 0\}$ Gesucht: $a \leq |H| - 1$ mit $\alpha^a := \underbrace{\alpha \circ \alpha \circ \dots \circ \alpha}_{a \text{ mal}} = \beta$

Anm. $\log_\alpha \beta$ sei schwer zu berechnen

Verallgemeinertes ElGamal Kryptosystem:

Schlüssel $K = (G, \alpha, a, \beta = \alpha^a)$

Verschlüsselung von x mit gewähltem zufälligem $k \in \mathbb{Z}_{|H|}$: $e_k(x,k) = (y_1, y_2)$

mit $y_1 = \alpha^k$, $y_2 = x \circ \beta^k$

Entschlüsselung $d_K(y) = y_2 \circ (y_1^a)^{-1}$

1. Alternative zu $\mathbb{Z}_p^*$: Galois-Körper

$\mathbb{Z}_p[x] / (f(x))$

Def $\mathbb{Z}_p[x]$: Menge der Polynome mit Variable x

$f(x)$ teilt $g(x)$ wenn es $q(x) \in \mathbb{Z}_p(x)$ mit $g(x) = q(x) f(x)$

$g(x) \equiv h(x) \pmod{f(x)}$ falls $f(x)$ teilt $(g(x) - h(x))$

besteht aus den Restklassen modulo $f(x)$

Jede Klasse hat einen Repräsentanten $r(x)$ mit $\deg(r) < \deg(f)$

Für $g(x)$ und $f(x)$ gibt es eindeutige $q(x), r(x)$ mit $g(x) = q(x) f(x) + r(x)$

$f(x) \in \mathbb{Z}_p[x]$ heißt irreduzibel falls keine $f_1(x), f_2(x)$ mit $f(x) = f_1(x) f_2(x)$ und $\deg(f_1) > 0$, $\deg(f_2) > 0$ existieren

$\mathbb{Z}_p[x] / f(x)$ ist ein Körper g.d.w. $f(x)$ irreduzibel ist.

$p = 2$

$f_1(x) = x^3 + 1 = (x+1)(x^2+x+1)$

$f_2(x) = x^3 + x + 1$ ✓

$f_3(x) = x^3 + x^2 + 1$ ✓

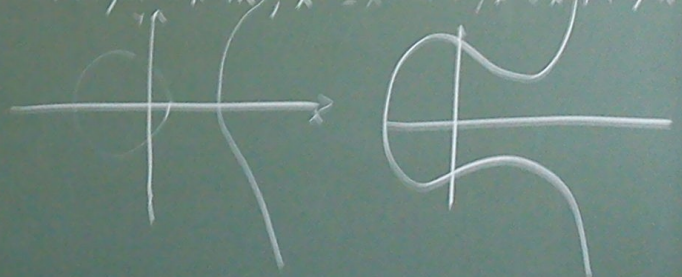
$f_4(x) = x^3 + x^2 + x + 1 = (x+1)(x^2+1)$

$\mathbb{Z}_2[x] / (x^3 + x + 1)$ ist Körper

$x, x^2, x^3 \equiv x+1, x^4 \equiv x^2 + x, x^5 \equiv x^2 + x + 1, x^6 \equiv x^2 + 1, x^7 \equiv 1$

2. Alternative: Elliptische Kurven

Sei $p > 3$ prim. Die elliptische Kurve $y^2 = x^3 + ax + b$ über $\mathbb{Z}_p$ ist definiert durch die Punkte $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ mit $y^2 \equiv x^3 + ax + b \pmod p$, wobei $a, b \in \mathbb{Z}_p$ mit $4a^3 + 27 b^2 \not\equiv 0 \pmod p$



$\mathcal{O}$ sei der unendlich entfernte Punkt

$P=(x_1,y_1)$, $Q=(x_2,y_2) \in E$ Wenn $x_2=x_1$ und $y_2=-y_1$ so ist $P+Q=\mathcal{O}$

sonst $P+Q=(x_3,y_3)$ mit $x_3=\lambda^2-x_1-x_2$, $y_3=\lambda(x_1-x_3)-y_1$

mit $\lambda=\begin{cases}\frac{y_2-y_1}{x_2-x_1} & \text{wenn } P\neq Q\\ \frac{3x_1^2+a}{2y_1} & \text{wenn } P=Q\end{cases}$

Bsp. $y^2=x^3+x+6$ über $\mathbb{Z}_{11}$

x	$x^3+x+6 \bmod 11$	$\in QR(11)$	$\mathbb{Z}_{11}$ y
0	6	—	
1	8	—	
2	5	✓	4, 7
3	3	✓	5, 6
4	10	—	
5	2	✓	2, 9
6	8	—	
7	4	✓	2, 9
8	9	✓	3, 8
9	7	—	
10	4	✓	2, 9

Wurzel kann berechnet werden als $\pm z^{(11+1)/4} \bmod 11$ $= \pm z^3 \bmod 11$

$\alpha=(2,7)$

$2\alpha=(2,7)+(2,7)$ $\lambda=(3\cdot 2^2+1)(2\cdot 7)^{-1} \bmod 11 = 8$

$x_3=8^2-2-2 \bmod 11=5$ $y_3=8(2-5)-7 \bmod 11=2$

$2\alpha=(5,2)$ $3\alpha=2\alpha+\alpha=(5,2)+(2,7)$

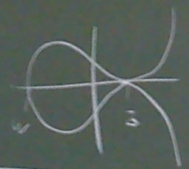
$\lambda=(7-2)(2-5)^{-1} \bmod 11=2$ $x_3=8$ $y_3=3$ $3\alpha=(8,3)$

$4\alpha=(10,2)$ $5\alpha=(3,6)$ $6\alpha=(7,9)$ $7\alpha=(7,2)$ $8\alpha=(3,5)$

$9\alpha=(10,9)$ $10\alpha=(8,8)$ $11\alpha=(5,9)$ $12\alpha=(2,4)$ $13\alpha=\mathcal{O}$

$p+1-2\sqrt{p} \leq \#E \leq p+1+2\sqrt{p}$

Es gibt n_1, n_2 mit n_2 teilt n_1 und n_2 teilt $(p-1)$, E ist isomorph zu $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$



$\Rightarrow$ $x^3+ax+b = (x-w)(x-z)^2 = -\underbrace{(w+2z)}_{0}x^2+\underbrace{(z^2+2wz)}_{a}x-\underbrace{wz^2}_{b}$

hat doppelte Nullstelle

$4a^3+27b^2 = 4\cdot(-3z^2)^3+27(2z^3)^2 = 4\cdot(-27)z^6+27\cdot 4z^6=0$ $a=-3z^2$ $b=2z^3$

Einsatz (naiv) für El Gamal

sei $\alpha=(2,7)$ und $a=7$ geheim, $\beta=2\alpha=(7,2)$

Verschlüsselung $e_k(x,k)=(k(2,7),\ x+k(7,2))$ $d_k(y_1,y_2)=y_2-7y_1$

Problem: Wie kann man eine natürliche Nachricht auf einen Punkt der Kurve abbilden

Nachteil: Darstellung ist 4 mal so groß wie die Nachricht

Menezes-Vanstone Elliptische Kurven Kryptosystem

$K = (E, \alpha, a, \beta = a \cdot \alpha)$ (a: geheim)

k zufällig aus $\mathbb{Z}_{|H|}$ Nachricht $x = (x_1, x_2) \in (\mathbb{Z}_p^*)^2$

$e_k(x, k) = (y_0, y_1, y_2)$ mit $y_0 = k\alpha$, $(c_1, c_2) = k\beta$, $y_1 = c_1 x_1 \bmod p$, $y_2 = c_2 x_2 \bmod p$

$d_k(y_0, y_1, y_2) = (y_1 c_1^{-1} \bmod p,\ y_2 c_2^{-1} \bmod p)$ mit $a \cdot y_0 = (c_1, c_2)$

Der Algorithmus von Shank-Tonelli kann auch für $p \equiv 1 \bmod 4$ Quadratwurzeln berechnen; allgemein ist Wurzel-ziehen modulo n effizient möglich wenn $\phi(n)$ bekannt ist.