PROPOSAL OF CRYPTOGRAPHIC ELLIPTIC CURVES GENERATOR

Daniel Herbrych
Master Degree Programme (2. year), FEEC BUT
E-mail: xherbr00@stud.feec.vutbr.cz

Supervised by: Radek Fujdiak
E-mail: fujdiak@feec.vutbr.cz

Abstract: This paper deals with creation of elliptic curves generator. The purpose is generating disposable elliptic curves for cryptographic protocol. Miracl library is used. The most important issue is to determine the order of the elliptic curve group. SEA algorithm (Schoof–Elkies–Atkin) is used for this purpose. The second goal is to find suitable elliptic curves for the cryptographic purposes.

Keywords: elliptic curves, on the fly, cryptography, group, schoof elkies atkins

1 ÚVOD

Kryptografie se dělí do dvou částí - symetrická a asymetrická. U symetrické kryptografie se používá jeden klíč jak pro šifrování, tak pro dešifrování. Před započetím komunikace je tedy třeba vyřešit distribuci klíče. Eliptické křivky spadají do asymetrické kryptografie. Asymetrické kryptosystémy se používají pro šifrování, podepisování a pro výměnu klíčů symetrických kryptosystémů. Eliptické křivky jsou typicky definovány různými institucemi, např. NIST. Eliptické křivky jsou perspektivní hlavně díky stejné úrovni zabezpečení při menších velikostech klíčů. Díky tomuto důvodu mají menší výpočetní nároky a je výhodné je použít obecně pro zařízení s omezenými zdroji, příkladem budiž IoT, karty atd. Alternativou k použití eliptických křivek, které už byly definovány nějakou institucí, je použití křivek vlastních. Tyto křivky mohou být generovány také pouze pro jednorázové použití, po kterém jsou tyto křivky zahozeny. Eliptické křivky jsou speciální podtřídou kubických křivek, čili polynomů třetího stupně. Obecně rovinnou křivkou rozumíme množinu bodů vyhovující rovnici [3]: $F(x,y) = 0$. Eliptické křivky jsou vždy definovány nad nějakým konečným polem $\mathbb{F}_q$, což ve výsledku vytvoří grupu. Operace jsou pak prováděny nad touto grupou. Eliptická křivka může být definována jako množina [3]:

$$E = \{[x,y] \in F_q^2 \setminus \{[0,0]\}, F(x,y) = 0\} \cup \{\infty\}, \tag{1}$$

kde jako dodatečný bod je třeba definovat tzv. bod v nekonečnu ∞, který úzce souvisí s řádem bodu. Nejmenší kladné celé číslo k tak, že $kP = \infty$, kde P je bod na křivce, se nazývá řád bodu P [3].

$$F(x,y) = y^2 + a_1xy + a_2y - x^3 - a_3x^2 - a_4x - a_5, \tag{2}$$

tato rovnice [3] je tzv. Weierstrassova forma pro eliptické křivky. Tato rovnice se dále zjednodušuje pro jednotlivá tělesa a upravují se podmínky pro koeficienty tak, aby křivka nebyla singulární. Singulární křivky jsou křivky mající nulový diskriminant a pro které je problém diskrétního logaritmu nad eliptickými křivkami redukován na klasický diskrétní logaritmus. V textu dále bude pracováno s prvočíselnými poli, čili $q = p$. U křivek nad prvočíselným polem $\mathbb{F}_p$ je cílem generovat parametry p,a,b,G,n,h. Parametr p je prvočíslo, společně s parametry a,b definuje křivku nad prvočíselným polem pomocí zjednodušené formy Weierstrassovy rovnice [3]:

$$y^2 \bmod p = x^3 + ax + b \bmod p. \tag{3}$$

Dále G je generátor (anglicky také base point), což je bod (x_G, y_G) vybraný pro další operace. Parametr n je řád generátoru. Skalár pro násobení bodů je pak vybírán z intervalu $\langle 0; n-1 \rangle$. Dalším parametrem je h neboli kofaktor, kde $h = \#E(\mathbb{F}_p)/n$. $\#E(\mathbb{F}_p)$ je počet počet prvků grupy nebo také řád grupy, někdy též kardinalita. Znak # pro označení počtu prvků množiny je používán např. ve [3]. Jedná se o tzv. kardinální číslo resp. kardinál, používá se namísto $|x|$. Kofaktor by měl mít nejlépe hodnotu 1, jinými slovy, aby generátor generoval všechny body grupy. V opačném případě, v závislosti na kofaktoru, bude generátor generovat podgrupu o řádu $\#E(\mathbb{F}_p)/h$.

2 NÁVRH GENERÁTORU

Samotné generování křivek zahrnuje několik kroků a způsobů generování je více. U křivek nad prvočíselným polem $\mathbb{F}_p$ se generují všechny parametry p, a, b, G, n, h. Nejčastějším způsobem je Algoritmus 1, což je už samotný generátor, jeho pseudokód je níže. Je velice podobný algoritmu generování z [1]. Vygenerováním náhodných parametrů a, b se definuje křivka nad určitým polem. Následně se určí řád grupy n, a to pomocí SEA algoritmu. Pak se najde vhodný generátor grupy a určit kofaktor už je snadné. Druhou nejčastější metodou je tzv. CM metoda (complex multiplication), která má na vstupu modulus p, výstupem je křivka a generátor. Její výhodou je větší rychlost než první způsob se SEA algoritmem, ale na druhou stranu výstupem jsou více strukturované křivky. Taktéž na implementaci je složitější. Použit je první uvedený způsob, který bude vysvětlen podrobněji. Jako první se zvolí modulus p, což je jeden z parametrů určujících výslednou grupu pro další operace. Modulus může mít různou délku v bitech a ta závisí na požadované úrovni zabezpečení. Druhým krokem je vygenerování náhodných parametrů a a b, které určují už samotnou eliptickou křivku. Zkontroluje se, zda pro generovanou křivku platí, že diskriminant není nulový. Pro diskriminant platí vztah [3]:

$$\Delta = -16(4a^3 + 27b^2). \tag{4}$$

Pokud je nulový, generují se nová a a b. Náhodný generátor konkrétně v tomto případě nemusí být opravdu náhodný, ale stačí pseudonáhodný. Tvar křivky totiž není tajný. V tomto bodě se vypočítá pomocí SEA algoritmu řád grupy nad danou eliptickou křivkou. Pro tento krok je použita knihovna MIRACL. Nyní se najde generátor, bod, který bude generovat podgrupu o dostatečně velkém řádu. K tomu se použije Algoritmus 2 uvedený níže. Pokud by kofaktor, neboli podíl řádu grupy a generované podgrupy, byl příliš velký, začíná se s novou křivkou. Platí [2]:

$$h = \#E(\mathbb{F}_p) \cdot r, \tag{5}$$

kde h je kofaktor, $\#E(\mathbb{F}_p)$ je označení řádu grupy nad eliptickou křivkou a r je velké prvočíslo reprezentující řád generované podgrupy. Nyní je třeba definovat zkratku MOV útok, a to dle pánů Menezes, Okamoto a Vanstone. Ti prezentovali redukci diskrétního logaritmu nad eliptickými křivkami na klasický diskrétní logaritmus, který lze řešit v subexponenciálním čase. MOV podmínka je naopak ochranou proti tomuto MOV útoku. Podmínka je splněna, pokud neexistuje žádné $k \in \{1, \ldots, B\}$ tak, že $\#E(F_p) | q^k - 1$. Hodnota B je kladné celé číslo zvané MOV threshold, které bývá voleno $B \geq 20$. Na závěr se zhodnotí, zda je tato grupa nad eliptickou křivkou vhodná pro kryptografické účely, to zahrnuje vyloučení anomálních křivek a kontrolu MOV podmínek. Anomální křivky patří do třídy křivek s určitými matematickými parametry, na které byl nalezen efektivní útok řešící problém diskrétního logaritmu nad eliptickými křivkami v lineárním čase. Co se týče počítání bodů na křivkách, čili SEA algoritmu, základem je Schoofův algoritmus z roku 1985. Základem algoritmu jsou tzv. dělicí polynomy a Frobeniův endomorfismus [3]:

$$\begin{aligned} \phi_p : E(\mathbb{F}_p) &\to E(\mathbb{F}_p), \\ (x, y) &\mapsto (x^p, y^p), \\ \infty &\mapsto \infty. \end{aligned} \tag{6}$$

Pro každý bod P platí rovnost [3]:

$$\phi_p^2(P) - t\phi_p(P) + pP = \infty, \tag{7}$$

kde $t = p + 1 - \#E(\mathbb{F}_p)$. Tato rovnost se nazývá charakteristická rovnice Frobeniova endomorfismu. Dále je známa Hasseho věta [3]:

$$|p + 1 - |E(\mathbb{F}_p)|| \leq 2\sqrt{p}, \tag{8}$$

která určuje meze, ve kterých se nachází počet prvků grupy eliptické křivky. Za pomoci Čínské věty o zbytcích se dokáže určit hledaný řád grupy eliptické křivky. Frobeniův endomorfismus, jeho charakteristická rovnice a Hasseho věta byly upraveny pro prvočíselná pole $\mathbb{F}_p$ namísto obecných polí $\mathbb{F}_q$. Níže jsou pseudokódy vybraných důležitých částí. Algoritmus 1 je kostra celého generování. Algoritmus 2 je způsob nalezení generátoru s velkým prvočíselným řádem.

Algoritmus 1 Generovani krivek nad $\mathbb{F}_p$

INPUT: modulus p
OUTPUT: usporadana sestice T,
kde $T = (p, a, b, G, r, h)$

1: $a =$ nahodne cislo
2: $b =$ nahodne cislo
3: **if** diskriminant je 0 **then goto** 1
4: $radKrivky =$ SEA(a,b,p)
5: **if** $radKrivky$ je p **then goto** 1
6: **if** kontrolaMOV není OK **then goto** 1
7: $r =$ nejvetsi cislo prvociselneho rozkladu
8: kofaktor $h = \#E(\mathbb{F}_p)/r$
9: **if** h je prilis velke **then goto** 1
10: nalezeni generatoru G
11: **return** T

Algoritmus 2 Nalezeni generatoru grupy

INPUT: usporadana petice $S = (p, a, b, r, h)$
OUTPUT: pokud rad krivky $\#E = hr$, pak generator radu r, jinak false

1: generovani nahodneho bodu P
2: bod $G = hP$
3: **if** G je bod v nekonecnu **then goto** 1
4: bod $Q = rP$
5: **if** Q neni bod v nekonecnu **then**
6: **return** false
7: **else**
8: **return** G

3 ZÁVĚR

Uvedený generátor bude použit v kryptografickém protokolu pro jednorázové generování eliptických křivek, tzv. on the fly. Křivka bude použita pouze jednou a zahozena. V protokolu bude křivky generovat osobní počítač představující server, klient bude zařízení Raspberry Pi 3 model B. Druhotně poslouží jako generátor pro měření efektivity různých eliptických křivek. V případě nalezení nějakého vzoru by to mohlo vést ke generování efektivnějších křivek a tím i ke zrychlení odpovídajících operací. Na potřebnost nových eliptických křivek také ukazuje jejich stávající nedostatečné množství.

REFERENCE

[1] BAIER, H.; BUCHMANN, J. *Generation Methods of Elliptic Curves*. Information-technology Promotion Agency. Japan. 2002.

[2] JOHNSON, D.; MENEZES, A.; VANSTONE, S. *The Elliptic Curve Digital Signature Algorithm (ECDSA)*. International Journal of Information Security. Certicom Research, Canada. Department of Combinatorics and Optimization, University of Waterloo, Canada. 2001.

[3] HANKERSON, D.; MENEZES, A.; VANSTONE, S. *Guide to Elliptic Curve Cryptography* Springer-Verlag New York, Inc., 2003, 332 s. ISBN 0-387-95273-X.