STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Isogenie v kryptografii

Zdeněk Pezlar
Jihomoravský kraj

Brno 2020

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Isogenie v kryptografii

Isogeny Based Cryptography

Autor: Zdeněk Pezlar
Škola: Gymnázium Brno, třída Kapitána Jaroše, p. o.
Kraj: Jihomoravský
Konzultant: Bc. Vojtěch Suchánek

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval samostatně a použil jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů. Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné. Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Brně dne: ..... Podpis: .....

jihomoravský kraj

Poděkování

++Tato práce byla vypracována za finanční podpory JMK.

Abstrakt

abstrakt

Klíčová slova

isogenie;klíčové slovo.

Abstract

abstrakt

Key words

isogenie;klíčové slovo.

Obsah

Úvod

celkem úvod

Použitá značení

$a \mid b$	a dělí b
$\mathcal{D}(a, b)$	největší společný dělitel a, b
$\left(\frac{a}{p}\right)$	Legendreův symbol a vzhledem k b
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	množina přirozených, celých, racionálních, reálných, komplexních čísel
$\mathbb{Z}_d$	okruh zbytků modulo d
$\mathbb{F}_q$	konečné těleso s q prvky
$\overline{\mathbb{F}}$	algebriacký uzávěr $\mathbb{F}$
$\mathbb{F}^\times$	multiplikativní podrupa $\mathbb{F}$
$\mathbb{F}^*$	$\mathbb{F} \setminus \{0\}$
$\mathbb{P}^n(K)$	projektivní prostor nad K o rozměru $n+1$
$R[x]$	okruh polynomů s koeficienty nad okruhem R
$K(a_1, \ldots, a_n)$	nejmenší podtěleso L, které obsahuje těleso K i prvky $a_1, \ldots, a_n \in L$
$\mathcal{O}_K$	okruh celých algebraických čísel tělesa K
$Cl(\mathcal{O}_K)$	grupa tříd ideálů tělesa K
h_K	řád grupy tříd ideálů tělesa K
(a)	hlavní ideál generovaný prvkem a
$\frac{\mathcal{I}}{m}$	lomený ideál $\frac{\mathcal{I}}{m}$
$\left(\frac{a}{m}\right)$	hlavní lomený ideál $\frac{(a)}{m}$
$N(a)$	norma prvku a
$N((a))$	norma ideálu generovaného a
$\mathcal{I} \mid \mathcal{J}$	ideál $\mathcal{I}$ dělí ideál $\mathcal{J}$
G/H	faktorgrupa G podle H
$f \in O(g)$	f roste asymptoticky nejvýše stejně rychle jako g
$f \in \Theta(g)$	f roste asymtoticky stejně rychle jako g
$f \in \Omega(g)$	f roste asymtoticky alespoň tak rychle jako g

Kapitola 1

Eliptické křivky

1.1 Základy

V naší první kapitole se budeme věnovat isogeniím eliptických křivek a práci s nimi. Budeme budovat teorii a intuici potřebnou k smysluplné diskuzi protokolu SIDH. Pro porozumění textu je třeba ovládat základy abstraktní algebry, viz [8]. Budeme postupovat vesměs dle [3], nicméně další vhodný úvodní materiál se nachází na [12]. Ne vždy budeme uvádět důkazy tvrzení, neboť jsou mnohdy příliš pokročilé či technické, v takových případech se odkážeme na relevantní literaturu.

Po celou dobu budeme pracovat nad projektivním prostorem nad uzávěrem tělesa K, což je množina bodů v $\overline{K}^n$, kde dva body považujeme za ekvivalentní, pokud leží v přímce s počátkem, můžeme proto místo jednotlivých bodů pracovat s přímkami skrz počátek. Chtěli bychom, aby se každé dvě $n-1$ rozměrné roviny protínaly, a s tím máme problém pouze pokud protínáme dvě rovnoběžné. V každém směru si tak můžeme definovat projektivní prostor stupně $n-1$ v nekonečnu, kde se protínají rovnoběžné roviny.

Definice 1.1.1. *Projektivní prostor $\mathbb{P}^n(\overline{K})$ definujeme jako množinu tříd nenulových vektorů $(a_0, \ldots, a_n) \in \overline{K}^{n+1}$ s ekvivalentní relací $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$, pokud existuje $\lambda \in \overline{K}$, že $(a_0, \ldots, a_n) = \lambda(b_0, \ldots, b_n)$. Tyto třídy ekvivalence budeme značit $(a_0 : \cdots : a_n)$.*

Pokud je jedno z a_i nulové, získáme $n-1$ rozměrný prostor v nekonečnu.

Projektivní prostor $\mathbb{P}^2(\mathbb{R})$ je známý jako projektivní rovina. Každé dvě přímky se protínají v jednom bodě, přičemž rovnoběžné přímky se protínají v bodě v nekonečnu v daném směru. Přímky procházející počátkem tak můžeme ztotožnit s jejich průsečíkem s rovinou neprocházíjí začátek, tedy každé takové přímce přiřadíme právě třídu, ve které leží její příslušný průsečík. Přímky s touto rovnou rovnoběžné, které v ní neleží, ji protínají v nekonečnu, a přiřadíme jim body v nekonečnu v jejich směru.

Poznámka 1.1.2. *Je zajímavé uvážit souvislost projektivních prostorů s barycentrickými souřadnicemi, kde je každý bod vyjádřen jako vážený průměr vrcholů referenčního simplexu.*

Tyto souřadnice jsou též homogenní a každé dvě přímky se protínají, byť některé v nekonečnu, takové body mají součet vah roven 0*. Můžeme tedy o barycentrických souřadnicích přemýšlet jako o projektivním prostoru s jiným základem.*

Přípomeňme si pak definici eliptické křivky. Často se definuje jako nesingulární projektivní křivka genu 1, pro naše účely si definici zúžíme.

Definice 1.1.3. *Mějme K těleso charakteristiky různé od* 2 *a* 3*. Pro $a, b \in K$, že $4a^2+27b^3 \neq 0$, definujeme v $\mathbb{P}^2(\overline{K})$ eliptickou křivku jako množinu bodů $(X : Y : Z) \in \overline{K}^3$ splňující:*

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Definice vylučující tělesa s charakteristikou 2 a 3 nám umožňuje zapsat křivku ve výše uvedené jednoduché formě. Avšak čtenář, jenž je již obeznámen s eliptickými křivkami, může protestovat, že eliptická křivka je množina bodů $x, y \in K$ splňující:

$$y^2 = x^3 + ax + b.$$

Pokud bod na eliptické křivky na přímce $Z = 0$, je i $X = 0$, a máme jediný bod $(0 : 1 : 0)$. Jinak můžeme celou rovnici podělit Z^3 a přejít na proměnné $x := \frac{X}{Z}, y := \frac{Y}{Z}$ a získat nám známou formu, kterou budeme dále označovat jako *afinní*, často se v literatuře uvádí jako *Weierstrassova*. Pak naše křivka je množina bodů $(x, y) \in \overline{K}^2$ splňujících $y^2 = x^3 + ax + b$ spolu s bodem v nekonečnu $\mathcal{O} = (0 : 1 : 0)$.

Definice 1.1.4. *Množinu všech bodů E nad konečným tělesem K (společně s $\mathcal{O}$) budeme značit $E(K)$ a počet jejích prvků budeme značit $\#E(K)$.*

Definice 1.1.5. *Pod bodem $P \in E$ budeme rozumět $P = (x, y) \in E(\overline{K})$.*

Podívejme se nyní na eliptickou křivku E geometricky, tedy v rovině vyznačme všechny body, které na ní leží. Je zjevné, že eliptická křvika je symetrická podle osy x, definujme proto k $P \in E$ opačný bod $-P \in E$ jako obraz P podle osy x. Pokud bychom na bodech naší křivky definovali součet, chtěli bychom, aby součet P a $-P$ byl $\mathcal{O}$.

OBrázky

Pokud řekneme, že tečna k E ji protíná ve dvou stejných bodech, pak každá přímka protíná E v právě třech bodech včetně multiplicity. Speciálně tečna v bodě s $y = 0$ tento bod protíná dvakrát a ten třetí je bod v nekonečnu E. Pak si sčítání $+$ na E můžeme definovat tak, že součet každých tří bodů v přímce je $\mathcal{O}$. Pokud tak přímka procházející $P, Q \in E$ protíná E potřetí v R, pak definujeme $P + Q = -R$. Pro součet bodů $P, Q \in E$ můžeme pak odvodit několik důležitých vlastností:

(i) $P + Q = Q + P$,

(ii) $(P + Q) + R = P + (Q + R)$,

(iii) $P + \mathcal{O} = P$,

(iv) $P + (-P) = \mathcal{O}$.

Při takto definovaném součtu můžeme s body na E pracovat jako s abelovskou grupou se sčítáním $+$ a neutrálním prvkem $\mathcal{O}$. Samozřejmě součet dvou bodů dokážeme za pomocí analytické geometrie přímo spočíst:

Věta 1.1.6. *Mějme afinní body $P = (x_1, y_1), Q = (x_2, y_2)$ s $P \neq -P$. Pak $P+Q = (x_3, y_3)$ je daný:*

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= -\lambda x_3 - y_1 + \lambda x_1, \end{aligned}$$

kde:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{pokud } x_1 \neq x_2, \\ \frac{3x_1^2 + a}{2y_1}, & \text{pokud } x_1 = x_2. \end{cases}$$

Důkaz s dovolením neuvádím. Pro zkrácení zápisu si budeme definovat skálární násobky bodů následovně:

Definice 1.1.7. *Mějme bod $P \in E$. Pak pro n přirozené definujeme jeho n-násobek:*

$$[n]_E P = \underbrace{P + \cdots + P}_{n},$$

příčemž pro $n < 0$ definujeme $[n]_E P = [-n]_E(-P)$ a $[0]_E P = \mathcal{O}$.

Pokud bude z kontextu jasné, nad kterou eliptickou křivkou pracujeme, budeme značit násobení skalárem pouze $[n]P$.

Příklad 1.1.8. *tu příklad sčítání, jak v Q tak v Fq, hezky graficky*

Příklad 1.1.9. *Určeme dvojnásobek bodu $P = (x, y)$ na $E : y^2 = x^3 + ax + b$.*

Řešení: V duchu značení věty 1.1.6 máme pro $[2]P = (x_1, y_1)$:

$$\begin{aligned} x_1 &= \lambda^2 - 2x = \frac{(3x^2 + a)^2}{4y^2} - 2x = \frac{(3x^2 + a)^2 - 8y^2 x}{4y^2} = \frac{(3x^2 + a)^2 - 8(x^3 + ax + b)x}{4(x^3 + ax + b)} \\ &= \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}, \\ y_1 &= -\lambda x_1 - y + \lambda x = -\frac{(3x^2 + a)[(3x^2 + a)^2 - 8y^2 x]}{8y^3} - y + \frac{x(3x^2 + a)}{2y} \\ &= \frac{(3x^2 + a)[-(3x^2 + a)^2 + 12y^2 x] - 8y^4}{8y^4} y \end{aligned}$$

$$= \frac{(3x^2+a)[-(3x^2+a)^2+12(x^3+ax+b)x]-8(x^3+ax+b)^2}{8(x^3+ax+b)^2}y$$
$$= \frac{x^6+5ax^4+20bx^3-5a^2x^2-4abx-a^3-8b^2}{8(x^3+ax+b)^2}y. \qquad \square$$

Všimneme si, že pro libovolný $P=(x,y)$ na eliptické křivce s $y=0$ je $[2]P=\mathcal{O}$. Pro bod $Q=(6,27):=(x_0,y_0)$ na křivce:

$$y^2=x^3+54x+189$$

nad $\mathbb{Q}$ zase ověříme, že:

$$x_0^6+5ax_0^4+20bx_0^3-5a^2x_0^2-4abx_0-a^3-8b^2=0,$$

tedy $[3]Q=\mathcal{O}$. Obecně by nás mohlo zajímat, které body pošle násobení n do nekonečna.

1.2 Torzní body

Definice 1.2.1. *Buď n celé číslo. O množině všech $P\in E$, že $[n]P=\mathcal{O}$, řekneme, že tvoří n-torzi E a tuto množinu budeme značit $E[n]$.*

Definice 1.2.2. *Buď P bod na E. Pokud n je nejmenší kladné číslo, že $[n]P=\mathcal{O}$, nazveme n řádem P. Pokud takové n neexistuje, řekneme, že P má nekonečný řád.*

n-torze na eliptické křivce E tvoří podgrupu $E(\overline{K})$, neboť pokud $[n]P=\mathcal{O}=[n]Q$, tak $[n]\,(P+\,Q)=[n]P\,+\,[n]Q\,=\,\mathcal{O}$. Torzní grupy nám pomáhají hlouběji studovat eliptické křivky v mnohých směrech. Například pro eliptickou křivku E nad konečným tělesem $\mathbb{F}_q$, je konečná grupa $E(\mathbb{F}_q)$ průnikem všech torzních podgrup, protože každý bod na E má konečný řád.

Zatímco $E(\mathbb{F}_q)$ je konečná grupa, grupa bodů na racionální křivce $E(\mathbb{Q})$ je nekonečná a existují i body nekonečného řádu. Příkladem mřížového bodu nekonečného řádu na křivce je bod $(70,13)$ na křivce:

$$E: y^2=x^3-13,$$

tedy jeho násobením můžeme získat nekonečně mnoho racionálních bodů na E. Body nekonečného řádu jsou obecně těžko spočitatelné, nicméně body s řádem konečným dokážeme všechny najít za pomocí věty Lutz-Nagella, [14, Thm. 8.7], dle které všechny takové racionální body (x,y) jsou mřížové a buď 2-torsní, či y^2 dělí diskriminant naší křivky.

Vraťme se k operaci násobení bodů. V poslední sekci našeho povídání o eliptických křivkách si u lemmatu 1.4.7 ukážeme, že $\deg[m]$, jakožto racionální funkce, je m^2. Díky [9, Exc. 3.30] ((((tohle bych asi chtěl rozepsat)))) můžeme proto říci:

Věta 1.2.3. *Nechť je E eliptická křivka nad K a m nenulové číslo. Pak:*

- *Pokud* $\operatorname{char} K \nmid m$*, tak* $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$*,*
- *Pokud* $p = \operatorname{char} K > 0$*:*

$$E[p^i] \cong \begin{cases} \{\mathcal{O}\}, & \text{pro každé nezáporné } i, \\ \mathbb{Z}_{p^i}, & \text{pro každé nezáporné } i. \end{cases}$$

Plný důkaz je k nalezení v: [9, Cor. III.6.4].

Vidíme, že existuje rodina křivek, která má pouze triviální p-torzi.

Definice 1.2.4. *Pokud máme* $E[p] \cong \{\mathcal{O}\}$*, nazveme* E *supersingulární. Jinak* E *budeme říkat obyčejná.*

Poznámka 1.2.5. *Algebraický uzávěr* $\mathbb{F}_p$ *je shodný s uzávěrem* $\mathbb{F}_{p^n}$ *pro každé* n*, neboť kořeny* $x^{p^n-1} - 1$ *jsou právě prvky* $\mathbb{F}_{p^n}^*$*, platí tedy* $\mathbb{F}_{p^n} \subseteq \overline{\mathbb{F}_p}$ *a* $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$*, z čehož vyvodíme* $\overline{\mathbb{F}_{p^n}} \subseteq \overline{\mathbb{F}_p}$ *a* $\overline{\mathbb{F}_p} \subseteq \overline{\mathbb{F}_{p^n}}$*. Neboť* n*-torze je množina* $P \in E(\overline{K})$*, že* $[n]P = \mathcal{O}$*, je supersingularita* E *nad* $\mathbb{F}_p$ *ekvivalentní její supersingularitě nad* $\mathbb{F}_{p^n}$*.*

Rozdělení křivek na obyčejné a supersingulární bude vhodné v mnoha ohledech, jak při diskuzi vlastností křivek, tak z kryptografického hlediska, k tomu však musíme hlouběji tyto křivky studovat.

Počítání celé p-torze je pro velká prvočísla výpočetně náročné, tudíž chceme najít vhodnější kritéria supersingularity. Uveďme proto pár ekvivalentních definic supersingularity křivky nad konečným tělesem:

Věta 1.2.6. *Nechť* E *je křivka nad* $\mathbb{F}_q$*, kde* $q = p^r$ *je mocnina prvočísla* $p > 3$*. Pak:*

$$\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$$

nastane právě pokud E *je supersingulární.*

Důkaz je k nalezení v [14, Prop. 4.31].

Věta 1.2.7. *Ať* E *je křivka nad* $\mathbb{F}_p$ *s* $p > 3$*. Pak:*

$$\#E(\mathbb{F}_p) = p + 1$$

nastane právě pokud E *je supersingulární.*

Důkaz je k nalezení v [14, Cor. 4.32].

Pro určení supersingularity E nás tak bude do jisté míry zajímat číslo $t = p+1-\#E(\mathbb{F}_p)$. Toto číslo je úzce spojené s jedním speciálním endomorfismem na E, který určuje mnoho vlastností samotné křivky. O tomto zobrazení se budeme podrobněji bavit v naší 3. kapitole.

Samotné počítání bodů na eliptické křivce je pro nás zatím obtížný, pro $\mathbb{F}_p$ s malým p můžeme jednoduše projít všechny možné hodnoty x, jak můžeme vidět na následujícím příkladu:

Příklad 1.2.8. *Ukažme, že křivka:*

$$E : y^2 = x^3 + 10x + 7$$

nad $\mathbb{F}_{13}$ *je supersingulární.*

Řešení: Pokud máme $(x, y) \in E(\mathbb{F}_{13})$, tak pro každé takové x existují dvě vyhovující y, pokud $x^3 + 10x + 7$ je v $\mathbb{F}_{13}$ nenulový čtverec, jedno, pokud je rovno nule, a jinak žádné. Můžeme si proto vypsat hodnoty pravé strany ve všech možných hodnotách a za pomocí Eulerova kritéria snadno určit, zda je výraz čtvercem, viz následující tabulka:

x	$x^3 + 10x + 7$	$\left(\frac{x^3+10x+7}{13}\right)$	počet řešení
0	7	-1	0
1	5	-1	0
2	9	1	2
3	12	1	2
4	7	-1	0
5	0	0	1
6	10	1	2
7	4	1	2
8	1	1	2
9	7	-1	0
10	2	-1	0
11	5	-1	0
12	9	1	2

U speciálních případů křivek můžeme rafinovaně využít poznatky z elementární teorie čísel:

Příklad 1.2.9. *Ukažme, že křivka:*

$$E : y^2 = x^3 + x$$

nad $\mathbb{F}_p$ *pro* $p \equiv -1 \pmod 4$ *je supersingulární.*

Řešení: Pro $p \equiv -1 \pmod 4$ je $\left(\frac{-1}{p}\right) = -1$, takže $p \mid a^2 + b^2 \Rightarrow p \mid a$ a $p \mid b$. Nenulových čtverců v $\mathbb{F}_p$ je právě $\frac{p-1}{2}$, tudíž každý prvek $\mathbb{F}_p$ je buď čtverec, nebo mínus čtverec. Pro $x = 0$ máme pouze $y = 0$ a pro každé $x \in \mathbb{F}_p^*$ je právě jedno z čísel $x^3 + x, (-x)^3 - x$ nenulovým čtvercem, protože je $x^2 \neq -1$. Pro každou dvojici $(x, -x)$ tak máme právě dvě řešení, dohromady $p-1$. Spolu s $(0, 0)$ a bodem v nekonečnu je $\#E(\mathbb{F}_p) = p+1$, díky větě 1.2.7 je E supersingulární. □

Díky poznámce 1.2.5 je křivka $E : y^2 = x^3 + x$ supersingulární nad konečným tělesem s charakteristikou $p \equiv -1 \pmod 4$.

Náš první postup počítání bodů na křivce běží nejlépe v $O(p)$ čase, což je pro prvočísla s $\log_2(p) > 500$, tedy prvočíslo praktické kryptografické velikosti, jednoduše příliš pomalé. Jedním z prvních velkých pokroků v počítání bodů byl *Schoofův algoritmus*, [10], který $\#E(\mathbb{F}_q)$ počítá v čase polynomiálním v $\log(q)$, což poskytzuje exponenciální zrychlení oproti našemu předchozímu způsobu.

případně rafinovaněji užít modulární aritmetiku, nicméně i to je polynomiální v p.

Pojďme se podívat na samotnou strukturu bodů na supersingulární E nad $\mathbb{F}_q$.

??
??

1.3 Zobrazení mezi eliptickými křivkami

Násobení bodů v E skalárem dává homomorfismus $E(\overline{K}) \longrightarrow E(\overline{K})$. Definuje proto endomorfismus na E daný lomenou funkcí nad K. My se nyní podíváme na zobrazení mezi jednotlivými eliptickými křivkami, konkrétně homomorfismy grup $E_1(\overline{K}) \longrightarrow E_2(\overline{K})$.

Uvažme zobrazení $(x, y) \mapsto (u^2x, u^3y)$, které převádí křivky:

$$E_1 : y^2 = x^3 + u^4ax + u^6b \mapsto E_2 : y^2 = x^3 + ax + b$$

pro libovolné $u \in \overline{K}$. To je lineární zobrazení mezi E_1 a E_2, které zachovává přímky a tedy i součet bodů na našich křivkách, definuje proto homomorfismus z $E_1(\overline{K})$ do $E_2(\overline{K})$. Navíc je zobrazení zjevně invertibilní, tudíž dokonce mezi $E_1(\overline{K})$ a $E_2(\overline{K})$ dává isomorfismus nad $\overline{K}$.

Věta 1.3.1. *(Sato-Tate) Dvě křivky E_1, E_2 nad konečným tělesem K jsou nad K isomorfní právě pokud $\#E_1(K) = \#E_2(K)$.*

Speciálně dvě křivky, které mají nad K pouze body v nekonečnu, jsou nad K isomorfní. Ne vždy máme nutně isomorfismus nad K, ale nad jeho rozšířením. Aby byl náš isomorfismus nad $\overline{K}$ definovaný, musí být díky předpisu $(x, y) \mapsto (u^2x, u^3y)$ nutně nad rozšířením K stupně dělícího 6.

Definice 1.3.2. *Buďte E, E' křivky isomorfní nad rozšířením K, ale ne nad K. Pak řekneme, že E' je twistem E nad K.*

Zobrazení z $E : y^2 = x^3 + ax + b$ dané $(x, y) \mapsto \left(\frac{x}{d}, \frac{y}{\sqrt{d^3}}\right)$ pro $\sqrt{d} \notin K, d \in K$, nám dává isomorfismus do:

$$E_d : y^2 = x^3 + d^2ax + d^3b,$$

avšak ne nad K, ale nad jeho kvadratickým rozšířením $K(\sqrt{d})$. E_d nazveme *kvadratickým twistem* E.

Pro křivky s $a = 0$, resp. $b = 0$, můžeme analogicky najít *kubický* a *sextický*, resp. *kvartický* twist:

$$y^2 = x^3 + b \mapsto y^2 = x^3 + d^2b,$$
$$y^2 = x^3 + b \mapsto y^2 = x^3 + db,$$
$$y^2 = x^3 + ax \mapsto y^2 = x^3 + dax,$$

dané po řadě $(x, y) \mapsto \left(\frac{x}{\sqrt[3]{d^2}}, \frac{y}{d}\right)$ a $(x, y) \mapsto \left(\frac{x}{\sqrt[3]{d}}, \frac{y}{\sqrt{d}}\right)$, resp. $(x, y) \mapsto \left(\frac{x}{\sqrt{d}}, \frac{y}{\sqrt[4]{d^3}}\right)$. Vidíme, že poslední dvě zmíněné křivky jsou navíc kvadratickými twisty po řadě kubického a kvadratického twistu E.

Chtěli bychom říci, kdy mezi dvěma eliptickými křivkami existuje isomorfismus, tedy najít nějaký invariant, který isomorfní křivky sdílí. Takovou funkci splňuje právě j-invariant.

Definice 1.3.3. *Pro eliptickou křivku $E : y^2 = x^3 + ax + b$ definujeme její j-invariant jako:*

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Poznamenejme, že ten je vždy nad K definovaný, neboť eliptické křivky mají nenulový diskriminant.

Věta 1.3.4. *Dvě křivky definované nad K jsou isomorfní nad $\overline{K}$ právě pokud mají stejný j-invariant.*

Mějme následujících pět křivek nad $\mathbb{Z}_{101}$:

$$E_1 : y^2 = x^3 + x + 1,$$
$$E_2 : y^2 = x^3 + 5x + 23,$$
$$E_3 : y^2 = x^3 + x - 1,$$
$$E_4 : y^2 = x^3 + 2,$$
$$E_5 : y^2 = x^3 + 2x.$$

Spočtěme si pak jejich j-invarianty nad $\mathbb{Z}_{101}$:

$$j(E_1) = 1728\frac{4}{31},$$
$$j(E_2) = 1728\frac{4 \cdot 5^3}{4 \cdot 5^3 + 27 \cdot 23^2} = 1728\frac{4 \cdot 24}{4 \cdot 24 + 27 \cdot 24} = 1728\frac{4}{31},$$
$$j(E_3) = 1728\frac{4}{31},$$
$$j(E_4) = 1728,$$
$$j(E_5) = 0.$$

Vidíme, že j-invarianty E_1 a E_2 se rovnají, přičemž v $\mathbb{Z}_{101}$ se oba rovnají $1728 \cdot 4 \cdot 88$, nutně mezi nimi existuje isomorfismus. Snadno ověříme, že zobrazení:

$$(x, y) \mapsto (3^2 x, 3^3 y) = (9x, 27y)$$

převádí:

$$\begin{aligned} y^2 = x^3 + x + 1 \qquad &\mapsto \qquad 27^2 y^2 = 9^3 x^3 + 9x + 1, \\ \Leftrightarrow \qquad &\qquad\quad 22y^2 = 22x^3 + 9x + 1, \\ \Leftrightarrow \qquad &\qquad\quad 22y^2 = 22x^3 + 110x + 506, \\ \Leftrightarrow \qquad &\qquad\quad\ \ y^2 = x^3 + 5x + 23. \end{aligned}$$

Inverzní isomorfismus $E_2 \longrightarrow E_1$ je pak daný $(x, y) \mapsto (34^2 x, 34^3 y) = (45x, 15y)$, neboť multiplikativní inverz 3 v $\mathbb{Z}_{101}$ je 34.

Křivka E_3 má ale též stejný j-invariant jako E_1 a E_2, nad $\mathbb{Z}_{101}$ mezi nimi a E_3 přesto isomorfismus neexistuje. E_3 je kvadratickým twistem E_1 nad $\mathbb{Z}_{101^2} = \mathbb{Z}_{101}[i]$, jakožto zobrazení $(x, y) \mapsto \left(\frac{x}{i^2}, \frac{y}{i^3}\right) = (-x, iy)$ převádí:

$$\begin{aligned} y^2 = x^3 + x + 1 &\mapsto -y^2 = -x^3 - x + 1, \\ \Leftrightarrow y^2 &= x^3 + x - 1. \end{aligned}$$

Dvě speciální hodnoty j-invariantu jsou 0 a 1728, kterých nabývají křivky, které mají po řadě lineární, resp. konstantní člen roven 0. Právě křivky s j-invariantem 0 mají kubický (a sextický) twist, ty s j-invariantem 1728 zase kvartický.

Mohli bychom si nicméně osvětlit, proč se v j-invariantu násobí číslem 1728. Důvodem jsou tělesa charakteristik 2 a 3, j-invariant se totiž klasicky definuje pro libovolnou nesingulární projektivní křivku genu 1, tj.:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

jako:

$$\frac{(b_2^2 - 24 b_4)^2}{\Delta},$$

kde Δ je diskriminant naší křivky a $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1 a_3$. Pro tělesa s $\operatorname{char} K \neq 2, 3$ můžeme definovat zobrazení, která převádí naši křivku na nám známý afinní tvar, detaily důkazu jsou k nalezení v [9, Ch. 3]. Obraz rovnice j-invariantu je právě takový, jak ho zde definujeme, násoben konstantou 1728.

Počet různých j-invariantů v $\overline{K}$ určuje počet tříd isomorfismů křivek nad $\overline{K}$, případně kterých hodnot j-invariant nikdy nenabude. Bohužel počet isomorfismů je nejvyšší možný, viz.:

Věta 1.3.5. *Pro každé $s \in \overline{K}$ existuje eliptická křivka E nad $K(s)$, že $j(E) = s$.*

Explicitní konstrukce pro $s \notin \{0, 1728\}$ takové křivky podána v [9, Prop. III.1.4 (c)] je:

$$y^2 + xy = x^3 - \frac{36}{s - 1728}x - \frac{1}{s - 1728},$$

přičemž díky $\operatorname{char} K \neq 2, 3$ můžeme tuto křivku zapsat ve Weierstrassově tvaru. Diskriminant této křivky jsme si nezmínili, neboť ho nepovažuji pro nás za důležitý.

S trochou více teorie pod naším opaskem, můžeme se hlouběji ponořit do světa supersingulárních křivek.

Věta 1.3.6. *Buď E supersingulární eliptická křivka nad $\mathbb{F}_p$. Pak $j(E) \in \mathbb{F}_{p^2}$.*

Důkaz v ?.

Věta 1.3.7. *Buď E eliptická křivka nad $\mathbb{F}_p$. Pak libovolná křivka E' nad $\mathbb{F}_p$ s $j(E) = j(E')$ je supersingulární právě pokud je E supersingulární.*

Věta 1.3.8. *Buď E supersingulární eliptická křivka nad $\overline{\mathbb{F}}$. Pak existuje E' nad $\mathbb{F}_{p^2}$, že $E \cong E'$.*

Věta 1.3.9. *Thm 54 v DeFeo.*

Jak násobení bodů E skalárem, tak braní twistu, jsou homomorfismy bodů křivek nad tělesem K, resp. jeho rozšířením. Spadají tak pod rodinu zobrazení eliptických křivek zvaných *isogenie*, o kterých se budeme dále bavit.

1.4 Isogenie

Definice 1.4.1. *Ať $E_1, E_2 \in \overline{K}$ jsou eliptické křivky. Surjektivní morfismus $\phi : E_1 \longrightarrow E_2$ daný racionální funkcí nad K, který posílá bod v nekonečnu E_1 na bod v nekonečnu E_2, nazveme isogenií. Pokud mezi E_1, E_2 existuje isogenie, nazveme je isogenní.*

Isogenie ϕ pak tedy definuje homomorfismus $E_1(\overline{K}) \longrightarrow E_2(\overline{K})$. Pokud naši isogenii uvážíme jako zobrazení:

$$\phi : E_1 \longrightarrow E_2 : (x, y) \mapsto (u(x, y), v(x, y))$$

pro u, v lomené funkce nad K, tak po substituci $(x, y) \mapsto (x/z, y/z)$, požadujeme, aby $(0 : 1 : 0) \mapsto (0 : 1 : 0)$.

Definice 1.4.2. *Pod stupňem isogenie ϕ budeme rozumět jejímu stupni jako lomené funkci v x, budeme značit* $\deg \phi$.

Stejně jako jsme se zabývali torzní podgrupou našich křivek, nebude překvapením, že bude pro studium isogenií důležité, které body zobrazí do nekonečna. Tyto body i v případě isogenií tvoří podgrupu $E(\overline{K})$.

Definice 1.4.3. *Pod jádrem isogenie ϕ rozumíme jádru ϕ jakožto homomorfismu grup $E_1(\overline{K}) \longrightarrow E_2(\overline{K})$. Značíme* $\ker\phi$ *a počet jeho prvků* $\#\ker\phi$.

S isogeniemi jsme se již na naší (prozatím) krátké cestě několikrát setkali, jak násobení skalárem, tak isomorfismy zmíněné na konci předchozí kapitoly, jsou isogeniemi. Násobení $[n]$ má z Véluových formulí stupeň n^2, isomorfismy jsou isogenie lineární a jejich jádry jsou po řadě $E[n]$ a $\mathcal{O}$. Zobrazení:

$$\phi : y^2 = x^3 + x \longrightarrow y^2 = x^3 + 11x + 62$$

mezi křivkami nad $\mathbb{Z}_{101}$ dané $(x, y) \mapsto \left(\frac{x^2+10x-2}{x+10}, \frac{x^2y+20xy+y}{x^2+20x-1}\right)$ je též isogenií, tentokrát stupně dvě. Jádrem ϕ je množina $\{\mathcal{O}, 10\}$, protože $x^2 + 20x - 1 = (x + 10)^2$ v $\mathbb{Z}_{101}$.

Jednou z nejdůležitějších isogeniích, o kterých se budeme bavit, je tzv. Frobeniův automorfismus.

Definice 1.4.4. *Buď $y^2 = x^3 + ax + b$ eliptická křivka nad konečným tělesem s charakteristikou p. Zobrazení:*

$$\pi : y^2 = x^3 + ax + b \longrightarrow y^2 = x^3 + a^p x + b^p,$$

dané:

$$(x, y) \mapsto (x^p, y^p),$$

se nazývá Frobeniovým endomorfismem.

Pevné body Frobeniova endomorfismu jsou právě prvky $\mathbb{F}_p$, tudíž pro lomenou funkci f nad $\mathbb{F}_p$ platí: $f(x_1^p, \ldots, x_n^p) = f(x_1, \ldots, x_n)^p$. Speciálně: $0^p = 0, 1^p = 1, a^p + b^p = (a + b)^p$ a $a^p \cdot b^p = (ab)^p$, tudíž Frobeniův endomorfismus je nad $\overline{\mathbb{F}_p}$ automorfismem.

n-tou mocninu Frobeniova endomorfismu definujeme jako $\pi^n : (x, y) \mapsto (x^{p^n}, y^{p^n})$, přičemž víme, že pevné body π^n jsou právě prvky $\mathbb{F}_{p^n}$, tedy π^n je automorfismem je právě nad $\mathbb{F}_q$, kde $q = p^k, k \leqslant n$.

Když již máme solidní představu pojmu isogenie, pojďme se nyní pobavit o několika jejich základních vlastnostech.

Věta 1.4.5. *Všechny isogenie $E \longrightarrow E$ spolu s $[0]$ tvoří se sčítáním $(\phi+\psi)P := \phi(P) + \psi(P)$ a skládáním $\phi \circ \psi := \phi(\psi)$ okruh, který budeme značit $End(E)$, a nazývat okruhem endomorfismů E.*

Neutrálním prvkem našeho okruhu pro sčítání je $[0]$ a pro kompozici zase $[1]$. Nyní pojďme zkoumat spojitost isogenie ϕ stupně n s isogenií $[n]$. Při definici isogenie jsme formualovali výrok „E je isogenní s E'“ jako ekvivalentní relaci. Každé isogenií totiž lze jednoznačně přiřadit její *duál*, jehož vlastnosti nám pomohou studovat jak samotnou isogenii, tak i $[n]$.

Věta 1.4.6. *Buď $\phi : E \longrightarrow E_1$ isogenie stupně n. Pak existuje jediná isogenie $\hat{\phi} : E_1 \longrightarrow E$, která pro každou jinou isogenii $\psi : E_1 \longrightarrow E_2$ splňuje:*

(i) $\phi \circ \hat{\phi} = [n]_{E'}$,

(ii) $\hat{\phi} \circ \phi = [n]_E$,

(iii) $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$,

(iv) $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$,

(v) $\hat{\hat{\phi}} = \phi$.

Isogenii $\hat{\phi}$ budeme označnovat jako isogenii duální k ϕ.

Důkaz v [9, Thm. III.6.1].

Lemma 1.4.7. *Platí:*

$$\widehat{[n]} = [n] \qquad a \qquad \deg[n] = n^2.$$

Důkaz: Zjevně $\widehat{[0]} = [0]$ a $\widehat{[1]} = [1]$, dále postupujme indukcí dle n. Za pomocí věty 1.4.6, (iv), máme:

$$\widehat{[n+1]} = \widehat{[n]} + \widehat{[1]} = [n] + [1] = [n+1].$$

Protože $[-1] : P \mapsto -P$ je isogenií stupně 1, je $[-1]$ též duálem sama sebe. Pak díky $[-1] \circ [n] = [-n]$ máme první část hotovou. Z definice sčítání máme $[m] \circ [n] = [mn]$, tudíž $[n] \circ \widehat{[n]} = [n^2]$. Dle věty 1.4.6, (i), je $[n]$ isogenií stupně n^2. □

Duální isogenie k ϕ je pak z našeho lemmatu též isogenií stupně n. Navíc pro libovolnou isogenii ϕ z E stupně n je $\ker\phi \subseteq \ker[n]$, neboť libovolný prvek v jádru ϕ se $\hat{\phi}$ pošle do nekonečna E.

Zaměřme se nyní na jádro isogenie.

Definice 1.4.8. *Mějme $E, E_1 \in \overline{K}$ a $\phi : E \longrightarrow E'$ isogenie stupně k. Pokud je $\#\ker\phi = k$, pak o ϕ řekneme, že je separabilní. Jinak řekneme, že ϕ je neseparabilní. V případě, že je $\deg\phi$ roven mocnině $\operatorname{char} K$, mluvíme o ϕ jako o čistě neseparabilní.*

Libovolný isomorfismus z E je separabilní, neboť má triviální jádro. Naopak Frobeniův automorfismus a pro supersingulární křivky i $[p]$ jsou isogenie čistě neseparabilní.

Věta 1.4.9. *Každá separabilní isogenie ϕ z E je, až na isomorfismus, jednoznačně určena svým jádrem. Pokud je tak $G = \ker \phi$ grupa tvořená jádrem ϕ, můžeme značit E/G cílovou křivku ϕ.*

Důkaz tvrzení je podán v [14, Prop. 12.12], nicméně autor využívá nástrojů Galoisovy teorie, jejíž znalost od čtenáře nepředpokládáme.

Separabilní isogenie z $E \longrightarrow E'$ je daná lomenou funkcí nad K a známe-li její jádro, dokážeme ji explicitně spočíst, přičemž libovolná podgrupa $E(\overline{K})$ je jádrem isogenie. Vzorce udávající (až na isomorfismus) přesný tvar separabilní isogenie z $E \longrightarrow E'$ s daným jádrem se nazývají *Véluovy* po Jeanu Véluovy, který je první publikoval roku 1971 ve [13]. Jejich zápis je obecně velmi nezáživný a pro nás je nepodstatný, stačí nám mít v povědomí, že separabilní isogenie s daným jádrem můžeme explicitně vyjádřit, jejich přesnou formu a důkaz správnosti jsou k nalezení v [2, Ch. 8.2]. V Sage 9.0 jsou Véluovy vzorce implementovány pro isogenii z E s jádrem G v $O(\#G)$ příkazem:

`EllipticCurveIsogeny(E,ker G)`,

Tvrzení 1.4.9 můžeme konkrétněji formulovat následovně:

$$(E/\langle A\rangle)/\langle B\rangle \cong (E/\langle B\rangle)/\langle A\rangle.$$

Kapitola 2

Uplatnění v kryptografii

Přes Caesarovu šifru až po šifrování za pomocí Enigmy v období druhé světové války, po většinu lidské historie se využívaly kryptografické systémy založené na faktu, že obě komunikující partie si po domluvě vyberou způsob maskování zprávy a ten pro ostatní zůstává skrytý. Příkladem je právě o kolik písmen v Caesarově šifře transponujeme. Tento způsob nutně závisí na faktu, že se obě strany před výměnou mají možnost přes bezpečný kanál na tomto způsobu domluvit. S přibývajícím počtem účastníků a frekvencí komunikace, na příklad našeho každodenního interagování na internetu, kde musí konverzace mezi všemi účastníky být bezpečná, je bohužel na úkor ceny přenosu třeba vyšší počet a velikost klíčů, a příbývá risk kompromitace.

Kvůli takovým obavám přišli Whitfield Diffie a Martin Hellman v roce 1976 s revolučním nápadem: asymetrickou kryptografií, kde každý z účastníků má svůj vlastní *privátní klíč*, který s nikým nesdílí. Všechny strany, i potenciální útočník, znají několik informací, které jsou známé jako *veřejné parametry*. Obě komunikující strany za pomocí veřejných informací tajně transformují svůj privátní klíč a výsledek, který budeme nazývat *veřejným klíčem*, publikují. Oba účastnící vezmou veřejný klíč toho druhého a provedou s ním ty samé tajné kroky závisící na jejich privátním klíči. Podstatou takové výměny je, že na jejím konci získají obě původní strany netriviální informaci, tedy informaci takovou, že žádná třetí strana ji nedokáže snadno uhodnout, za pomocí níž poté mohou společnou komunikaci šifrovat a nikdo jiný již jejich zprávy neuvidí. Předpokládá se, že pouze ze znalosti veřejného klíče je pro každou další partii těžké replikovat klíč privátní a že pole možných sdílených informací je obrovské. Vyhneme se tak přímočarým řešením hrubou silou.

Pojďme se podívat na protokol, který Diffie a Hellman navrhli. Budeme o něm dále mluvit jako o *Diffie-Hellmanově výměně*. Je založena na problému *diskrétního logaritmu* prvku $a \in \mathbb{Z}_p^*$. Tento problém po nás ze znalosti primitivního kořene g modulo p žádá najít k, že $g^k = a$ v $\mathbb{Z}_p$. Obecně můžeme $\mathbb{Z}_p$ nahradit cyklickou grupou G a mít g její generátor. Protokol požaduje, aby nebyl diskrétní logaritmus spočitatelný efektivně, tj. v polynomiálním čase vzhledem k velikosti grupy, jinak může útočník jednoduše privátní klíče obou stran spočíst, ale mocnění bylo. Umocnit číslo dokážeme v logaritmickém čase, a v konečné grupě

nám stačí umocnit pouze na exponent modulo řádu grupy.

Veřejné parametry: Grupa G řádu p, kde p je prvočíslo, s generátorem g.

Alfréd		Blažena
Vstup: $a \in G^*$		**Vstup:** $b \in G^*$
	$\xrightarrow{g^a}$	
	$\xleftarrow{g^b}$	
$G_{AB} := \left(g^b\right)^a = g^{ab}$		$G_{BA} := \left(g^a\right)^b = g^{ba}$
Výstup: G_{AB}		**Výstup:** G_{BA}

Algoritmus 1: Diffie-Hellmanova výměna

Díky předpokladu, že G je cyklická, je i abelovská, tedy $G_{AB} = g^{ab} = g^{ba} = G_{BA}$. Na konci protokolu tak mají obě strany shodné tajemství g^{ab}.

Řád G se prakticky bere prvočíslo $q = 2p + 1$, že p je prvočíslo, p nazveme tzv. *Sophie-Germainovým prvočíslem* a q zase *bezpečným prvočíslem*. V takovém případě má G podgrupu prvočíselného řádu p, což je z kryptografického hlediska žádané, je tuto grupu totiž obtížnější spočíst. Navíc bezpečná prvočísla skýtají i výhody pro inicializování výměny, pro taková prvočísla dokážeme totiž snadno nalézt primitivní kořen. Konkrétně, g je primitivní kořen modulo $2p + 1$, tedy má řád $q - 1 = 2p$ modulo q, právě pokud $g^p \equiv -1 \pmod{q}$. Stačí nám pak najít $g^p \pmod{q}$, což nám mohou usnadnit nástroje jako Eulerovo kritérium, díky kterému je postačující mít g kvadratický nezbytek modulo q.

Veřejné klíče g^a, g^b, jsou nicméně, jak jejich název napovídá, veřejné, a má k nim přístup libovolná jiná osoba. Dejme tomu, že Eva, která má přístup pouze k veřejně dostupným informacím G, g, g^a, g^b, by chtěla též znát sdílené tajemství. Jeden způsob, jak by mohla tajnou informací získat, je pokud by spočítala diskrétní logaritmus $\log_g(g^a) = a$, nicméně předpokládáme, že to je obtížné. Na klasických počítačích jsou nejlepší známé útoky na problémy, jako diskrétní logaritmus a faktorizace čísla, na čemž jsou založené protokoly jako RSA, subexponenciální, nicméně na počítačích kvantových jsou už od poloviny 90. let známé algoritmy polynomiální. V čem však takto podstatné zrychlení spočívá?

2.1 Kvantové počítače

If computers that you build are quantum,
Then spies of all factions will want 'em.
Our codes will all fail,
And they'll read our email,
Till we've crypto that's quantum, and daunt 'em.

Jennifer a Peter Shorovi

Při diskuzi moderní kryptografie se často zmiňuje, že kvantové počítače dokáží problémy, jako faktorizaci čísla či diskrétní logaritmus, vyřešit v polynomiálním čase, přičemž nejrychlejší známé algoritmy pro klasické počítače pracují v čase subexponenciálním. V čem ale takto podstatné zrychlení spočívá?

Ve světě kvantových obvodů místo s klasickými bity pracuje s *qubity*. V n bitovém systémů máme 2^n různých stavů, které v n qubitovém systému tvoří generátory našeho prostoru. Podstatou je, že před pozorováním nemá daný qubit jednu z těchto hodnot, ale jejich (komplexní) superpozici. Generátory systému s jedním qubitem jsou stavy $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$, systém je tedy:

$$\alpha|0\rangle + \beta|1\rangle,$$

kde α, β jsou komplexní čísla $|\alpha|^2 + |\beta|^2 = 1$. Zápis $|\psi\rangle$ je tzv. *ket* notace, kde ψ je vektor.

V dvojqubitovém systému máme čtyři báze a stav takového systému je:

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,$$

kde $\alpha, \beta, \gamma, \delta$ jsou komplexní čísla s $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Qubity jsou značně nestabilní, musí být uchovány v izolované soustavě, nejčastěji v neutrinu, přičemž jakékoli narušení, i pouhé pozorování hodnoty qubitu, ho kolapsuje na jednu hodnotu, kterou už pak zůstane. Při pozorování má qubit pravděpodobnost ukázat stav právě takovou, kolik je druhá mocnina absolutní hodnoty příslušného koeficientu, proto ona normalizační podmínka. Pokud bychom pozorovali náš jedno-qubitový systém, s pravděpodobností $|\alpha|^2$ získáme výstup 0, s pravděpodobností $|\beta|^2$ získáme 1.

Můžeme ale též náš qubit vyjádřit ve vektorovém zápisu:

$$|\psi\rangle = \begin{bmatrix}\alpha\\\beta\\\gamma\\\delta\end{bmatrix},$$

což samozřejmě zobecníme pro systémy více qubitů. Tento vektor je díky naší podmínce jednotkový. V klasických obvodech máme brány, které jsou lineární zobrazení našich stavů, příklady takových bran jsou OR a NOT. V kvantových obvodech bereme jako brány právě unitární matice a jejich operaci násobení, neboť ty zachovávají normu vektoru, jejich výsledky jsou proto opět qubity.

Nedá moc práce ukázat, že všechny operace proveditelné na klasickém obvodu jsou replikovatelné kvantovými branami, model kvantového počítače, jakožto obvodu, je tak alespoň stejně silný jako počítač klasický.

Jedním z důvodů, proč se věří, že s veřejně dostupnými kvantovými počítači přijde nová éra výpočetní techniky je, že existují procesy, o kterých se dodnes neví, zda jsou v polynomiálním čase proveditelné na počítači klasickém, a jejichž kvantové algoritmy již byly nalezené. Klasické násobení čísel (n bitových), zabere $O(n^2)$ klasických operací, případně až $O(n^2 \log n)$ pro velká čísla, neboť jejich násobení neprovedeme v konstantním čase. Násobení dvou čísel se dá redukovat na problém násobení dvou polynomů, přičemž diskrétní Fourierova transformace z našeho polynomu nám dá informaci o hodnotách polynomu v odmocninách z jednotky, což je vše, co potřebujeme k určení polynomu. Rychlá Fourierova transformace toto dokáže pouze v $\Theta(n \log n)$ čase. Díky její multiplikativitě, linearitě a její inverzní funkci pak dokážeme zpětně v tomto čase získat součin dvou čísel.

Kvantová Fourierova transofrmace (QFT), která obdobnou operaci aplikuje na náš vektor, na klasickém počítači s n qubity počítá s 2^n prvky a nejlepší známé algoritmy ji provádí v $O(n^2 2^n)$ čase, zatímco na kvantových počítačích pracuje v kvadratickém čase a s jistou přesností i v $\Theta(n \log n)$, viz [1, Ch. 4. a 5.] pro více informací. Vynásobit dvě matice řádu n na klasickém počítači zjevně nedokážeme rychleji než $\Omega(n^2)$, neboť musíme pracovat se všemi n^2 prvky matice. Kvantový počítač dokáže dvě matice řádu n vynásobit užitím $O(n^{5/3})$ kvantových bran.

Faktorizaci celého čísla dokážeme snadno převést na problém hledání řádu čísla a modulo n. V devadesátých letech minulého století přišel Peter Shor s polynomiálním řešením

2.2 SIDH — Supersingular Isogeny Diffie-Hellman

Nyní, když jsme již trochu obeznámeni s kvantovými algoritmy, vraťme se zpět k eliptickým křivkám. Zjevnou adaptací Diffie-Hellmanova protokolu je protokol, který nese název ECDH (Elliptic Curve Diffie-Hellman):

Veřejné parametry: Prvočíslo p a eliptická křivka E nad $\mathbb{Z}_p$ s generátorem $G \in E(\mathbb{Z}_p)$.

Alfréd		Blažena
Vstup: $a \leqslant \#E(\mathbb{Z}_p) - 1$		**Vstup:** $b \leqslant \#E(\mathbb{Z}_p) - 1$
	$\xrightarrow{[a]G}$	
	$\xleftarrow{[b]G}$	
$G_{AB} := [a]([b]G) = [a][b]G$		$G_{BA} := [b]([a]G) = [b][a]G$
Výstup: G_{AB}		**Výstup:** G_{BA}

Algoritmus 2: Protokol ECDH

Tento protokol je založen na předpokladu, že diskrétní logaritmus na eliptických křivkách, tedy ze znalosti P a $[n]P$ spočíst n, je těžký problém. Není znám žádný algoritmus, který by

nezískal společné tajemství výpočtem privátních klíčů obou stran. Nicméně neboť $E(\mathbb{Z}_p)$ je konečná grupa, na kvantovém počítači je diskrétní logaritmus spočitatelný v čase polynomiálním ?

Pojďme se nyní znovu podívat na větu 1.4.9. Vidíme, že křivky $\phi(\psi(E)), \psi(\phi(E))$ sdílí j-invariant, neboť jsou isomorfní, což by v potenciálním protokolu založeném na isogeniích mohlo být sdílené tajemství obou stran. Pokud tak mají obě strany danou křivku E nad $\overline{\mathbb{F}_q}$, vyberou si tajné isogenie ϕ_A, resp. ϕ_B, pošlou druhé straně $\phi_A(E)$, resp. $\phi_B(E)$ a obě strany již snadno spočtou své tajemství. Takové myšlenky měli De Feo a Jao v [?], nicméně než se dostaneme přímo k jejich navrhovaném protokolu SIDH, musíme diskutovat několik důležitých detailů, které se vyhýbají známým útoků, případně usnadňují výměnu.

Jak napovídá název protokolu, požadujeme supersingularitu E. Pak totiž z věty 1.2.6 je $\#E(\mathbb{F}_{p^2}) = p + 1$ a $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$. Pro prvočíslo $p = \ell_A^{e_A}\ell_B^{e_B} - 1$, kde ℓ_A, ℓ_B jsou prvočísla, proto existují dva body G_1, G_2 řádu $\ell_A^{e_A}\ell_B^{e_B}$, které generují $E(\mathbb{Z}_{p^2})$. Speciálně dvojice $\langle P_A, Q_A\rangle := \langle [\ell_B^{e_B}]G_1, [\ell_B^{e_B}]G_2\rangle$, resp. $\langle P_B, Q_B\rangle := \langle [\ell_A^{e_A}]G_1, [\ell_A^{e_A}]G_2\rangle$, generují po řadě $\ell_A^{e_A}$, $\ell_B^{e_B}$ torzi.

Uvažme bod $P \in E[\ell_A^{e_A}]$ řádu ℓ_A^t a separabilní isogenii $\phi : E \longrightarrow E/\langle P\rangle$. Pokud bychom chtěli $E/\langle P\rangle$ spočíst, stačilo by spočítat celou $\langle P\rangle$ a za pomocí Véluových formulí spočíst výslednou křivku v čase $O(\ell_A^t)$, což zjevně není optimální.

Veřejné parametry: Grupa G řádu p, kde p je prvočíslo, s generátorem g.

Alfréd		Blažena
Vstup: $a \in G$		**Vstup:** $b \in G$
	$\xrightarrow{g^a}$	
	$\xleftarrow{g^b}$	
$G_{AB} := \left(g^b\right)^a = g^{ab}$		$G_{BA} := \left(g^a\right)^b = g^{ba}$
Výstup: G_{AB}		**Výstup:** G_{BA}

Algoritmus 1: Diffie-Hellmanova výměna

Kapitola 3

Algebraická teorie čísel

Ve snaze vybudovat teorii k hlubšímu studiu eliptických křivek a isogenií, natož diskuzi protokolu CSIDH, musíme samozřejmě někde začít, od čtenáře následujících sekcí se proto předpokládá znalost základu algebraické teorie čísel. Jako podrobné materiály ke studiu této krásné oblasti matematiky vřele doporučuji [4], [8]. Jako decentní stručný úvod motivovaný poznatky z elementární teorie čísel může též posloužit má SOČ [6, kap. 2].

Připomeňme si několik pár základních faktů ohledně tříd ideálů okruhu $\mathcal{O}$

Závěr

zu ende

Literatura

[1] Chuang, Isaac L. a Nielsen, Michael A.: *Quantum computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[2] De Feo, Luca.: *Fast Algorithms for Towers of Finite Fields and Isogenies*. EcolePolytechnique X, 2010.

[3] De Feo, Luca.: *Mathematics of Isogeny Based Cryptography*. Université de Versailles & Inria Saclay, 2017. Dostupné z: https://arxiv.org/abs/1711.04062.

[4] Marcus, Daniel A.: *Number fields*. New York: Springer-Verlag, 1977.

[5] Matushak, Andy a Nielsen, Michael A.: *Quantum computing for the very curious*. San Francisco, 2019. Dostupné z: https://quantum.country/qcvc.

[6] Pezlar, Zdeněk: *Zajímavá využití algebraické teorie čísel*. Středoškolská odborná práce. Brno, 2020.

[7] Raclavský, Marek: *Racionální body na eliptických křivkách*. Diplomová práce. Praha, 2014.

[8] Rosický, Jiří: *Algebra*. Brno: Masarykova univerzita, 2002.

[9] Silverman, Joseph H.: *The Arithmetic of Elliptic Curves*. New York: Springer-Verlag, 1992.

[10] Schoof, René: *Elliptic Curves Over Finite Fields and the Computation of Square Roots* $\bmod p$. J. Théor. Nombres Bordeaux 7 Dostupné z: https://www.ams.org/journals/mcom/1985-44-170/S0025-5718-1985-0777280-6/S0025-5718-1985-0777280-6.pdf.

[11] Shor, Peter W.: *Polynomial-Time Algorithms for Prime Factorizationand Discrete Logarithms on a Quantum Computer*. New York: Springer-Verlag, 1994. Dostupné z: https://arxiv.org/abs/quant-ph/9508027.

[12] Sutherland, Andrew V.: *Elliptic Curves*. Massachusetts Institute of Technology, 2017. Dostupné z: https://math.mit.edu/classes/18.783/2017/lectures.html.

[13] Vélu, Jacques: *Isogénies entre courbes elliptiques*.Comptes Rendus de l'Académie des Sci-ences de Paris, 1971. Dostupné z: https://math.mit.edu/classes/18.783/2017/lectures.html.

[14] Washington, Lawrence C.: *Elliptic Curves: Number theory and cryptography*. Maryland, 2008.