УНИВЕРЗИТЕТ ЦРНЕ ГОРЕ

Природно-математички факултет Подгорица

Иванка Пипер

ЕЛИПТИЧНЕ КРИВЕ И ЊИХОВА ПРИМЈЕНА У КРИПТОГРАФИЈИ

СПЕЦИЈАЛИСТИЧКИ РАД

Подгорица, 2021.

УНИВЕРЗИТЕТ ЦРНЕ ГОРЕ

Природно-математички факултет Подгорица

ЕЛИПТИЧНЕ КРИВЕ И ЊИХОВА ПРИМЈЕНА У КРИПТОГРАФИЈИ

СПЕЦИЈАЛИСТИЧКИ РАД

Криптографија

Ментор: Владимир Божовић

Иванка Пипер

Студијски програм: Математика и рачунарске науке

Подгорица, фебруар 2021.

Посвета

Захваљујем се професору Владимиру Божовићу на несебичној помоћи приликом писања овог рада. Такође се захваљујем мојим најмилијима. Сваки свој успјех дугујем њима, с тога им посвећујем овај рад.

Апстракт

Циљ овог рада је резимирање основних теоријских својстава елиптичних кривих која су неопходна за примјену у криптографији. Такође, у овом раду биће објашњене примјене елиптичних кривих у алгоритмима за размјену криптографских кључева, као и у алгоритмима за дигитално потписивање. На крају ће бити представљени савремени сигурносни протоколи чија се безбједност заснива на системима који користе елиптичне криве. Примјена елиптичних кривих која ће бити представљена у раду значајно је подигла ниво безбједности шифрованих података.

Abstract

The aim of this research is to summarize just enough of the basic theory of elliptic curves for their application in cryptography. Also, in this paper will be explained applications of elliptic curves in the algorithms for exchanging cryptographic keys and algorithms for the digital signature. At the end, modern security protocols whose security is based on systems that use elliptic curves will be presented. The application of elliptic curves in cryptography, which will be discribed in this paper significantly raises the level of security of encrypted data.

Садржај

Глава 1

Увод

Од давнина постојала је потреба за заштитом одређених података. Проблем заштите података није искључиво питање савременог доба. Тачно вријеме и мјесто у којем је настала криптографија као наука није познато. Прве, конкретне примјене, налазимо у Египту 2000 г.п.н.е гдје су кориштени нестандардни хијероглифи. Током историје шифровање података се користило првенствено у војне сврхе. Тако је настао чувени принцип шифровања римског владара Јулија Цезара. У Античкој Грчкој био је развијен чувени систем шифровања „Скитале". Италијански архитекта Леоне Батиста Алберти је 1467. године написао прву познату расправу о криптографији. Он је и творац такозваног шифрарског круга и неких других рјешења двоструког прикривања текста која су у 19. вијеку прихватили и усавршавали еминентни шифрантски бирои. Временом су развијани све бољи математички модели који су касније претварани у алгоритме на којима се заснива криптографија. Све до Другог свјетског рата шифроване поруке могле су се дешифровати. Њемци су, назвавши је Енигма, изумили машину која је шифровала податке на до тада непознат начин. Ипак савезници су нашли начин да разбију поруке шифроване Енигмом.

Развојем савремених средстава комуникације и трговине јављају се нови проблеми очувања безбједности информација и средстава које се преносе комуникационим каналима, што условљава стални развој криптографских алгоритама, који су основа заштите сваке мреже од спољних напада. Данас, криптографски алгоритми се дијеле у двије основне категорије, то су симетрични и асиметрични. Како су се појављивали рачунари са све бољим перформансама, радећи по неколико стотина, а касније и милиона операција у секунди, омогућено је пробијање шифри за све мање времена. Упоредо с тим, радило се и на измишљању нових, сигурнијих и компликованијих алгоритама за шифровање.

Криптографија је наука о заштити шифроване информације. Четири основна циља криптографије су: интегритет и вјеродостојност података који се шифрују, тајност података, аутентичност извора података и непорецивост. Данас се у примјени налази значајан број криптографских метода. Једна од метода која посједује одређене предности и недостатке је заснована на кориштењу елиптичних кривих. Елиптичне криве су глатке алгебарске криве[1] које су се почеле примјењивати у криптографији захваљујући Нилу Коблицу и Виктору Милеру. Почетком 21. вијека елиптичне криве су нашле ширу употребу у криптографији. Данас имамо мноштво развијених криптографских система који користе елиптичне криве. По неким истраживањима се показало да пружају исти ниво сигурности за чак 7 пута краће кључеве у односу на неке друге алгоритме, да имају мање захтјеве за меморијским капацитетима али су исто тако спорији.

У овом раду говориће се о неким основним појмовима у криптографији. Затим ће бити уведен појам елиптичне криве и биће обрађена основна својства која су потребна за бављење криптографијом која је базирана на њима. У скупу

[1]Алгебарске криве представљају скуп тачака у равни које се могу дефинисати алгебарским изразом $f(x, y) = 0$.

тачака елиптичне криве биће обрађен проблем дискретног логаритма као и дигиталог потписивања. Поред тога биће ријечи о неким савременим протоколима за заштиту комуникације и података на интернету који користе криптографске методе базиране на елиптичним кривим.

Глава 2

Основни појмови у криптографији и криптографски ситеми

Криптографија[1] је научна дисциплина која се бави начинима и методама очувања тајности информација. Упоредо са развојем криптографије развила се и **криптоанализа** - наука која се бави анализом шифроване информације како би разбила криптографску заштиту и дошла до оригиналне информације.

Криптологија је наука која обухвата криптографију и криптоанализу. Криптологија се бави проучавањем поступака за шифровање и дешифровање информација.

Енкрипција је процес у којем се помоћу специјалног **алгоритма енкрипције** податак или порука трансформише у криптограм(шифровани текст). Процес супротан процесу енкрипције, назива се **декрипција**. Да би се процес енкрипције и декрипције реализовао неопходно је имати податак који се назива **кључ**.

Криптосистем чине криптографски алгоритми (енкрипције и декрипције),

[1]Сама ријеч криптографија потиче од грчких ријечи *kryptos*, што значи скривено и *grafo*, што значи писање.

скуп изворних и криптованих података и скуп или домен кључа. Заштита шифрованих података у многоме зависи од заштите кључа. У односу на начин коришћења кључа, развиле су се двије класе криптографских система, **симетрични** и **асиметрични**.

2.1 Симетрични криптографски системи

Од античког доба па до седамдесетих година прошлог вијека криптографија је била заснована искључиво на овој методи. Данас такође има широку примјену за шифровање података и провјеру интегритета поруке.

Код симетричних криптографских система исти кључ се користи за процесе енкрипције и декрипције. Иако се некада заједно са кључем чувао у тајности, показало се да скривање самог алгоритма не доприноси повећању сигурности па су данас познати сви савремени симетрични алгоритми. Како криптографски кључ представља дијељену тајну у процесу комуникације велики недостатак ове врсте алгоритама се огледа у томе да уколико у току комуникације нападач открије кључ он може сам шифровати и дешифровати поруке што би представљало нарушавање основних сигурносних циљева у комуникацији.

Посматрано математички, процесе енкрипције и декрипције можемо описати на следећи начин:

$$C = E_k(M)$$

$$M = D_k(C)$$

гдје је E функција енкрипције, D функција декрипције, k тајни кључ, јединствен за обије стране, M оригинална порука[2], а C одговарајућа шифрована порука[3].

[2]ен. *plaintext*
[3]ен. *ciphertext*

Сви симетрични криптографски системи, према величини изворне поруке над којом се примјењује алгоритам енкрипције или декрипције, дијеле се у двије групе, и то:

- Секвенцијални или низ криптографски системи
- Блок криптографски системи

У наредним потпоглављима ће бити детаљније обрађена ова два типа криптографских система.

2.1.1 Секвенцијални криптографски системи

Као што и сама ријеч каже, секвенцијални (низ) криптосистеми врше енкрипцију бит по бит. Основна идеја овог криптографског система је да се бинарни низ који се шифрује сабере по модулу два са криптографским кључем.

Дефиниција 2.1 (Низ криптосистем)**.** *На сваки бит x_i поруке $m = (x_1, x_2, ..., x_n)$ се сабере по модулу* 2 *одговарајући бит k_i из низа који представља тајни кључ $k = (k_1, k_2, ...k_n)$.*

***Енкрипција**:*

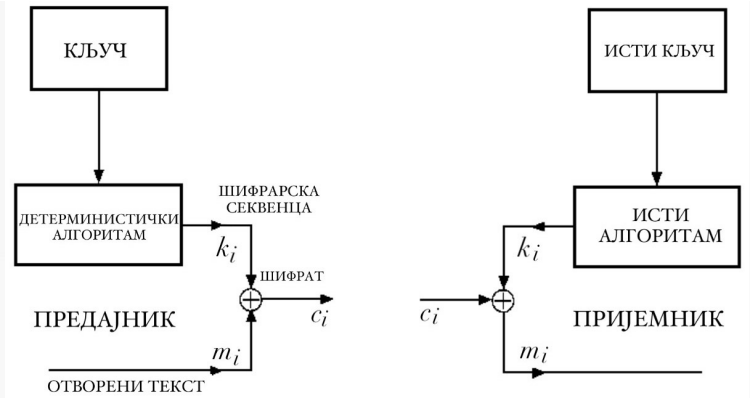
$E_k(m) = (x_1 \oplus k_1, x_2 \oplus k_2, ..., x_n \oplus k_n) = (c_1, c_2, .., c_n) = c.$

***Декрипција**:*

$D_k(c) = (c_1 \oplus k_1, c_2 \oplus k_2, ..., c_n \oplus k_n) = (x_1, x_2, .., x_n) = m.$ *[1]*

Случајни низ који се дефинише неким алгоритмом се назива псеудослучајни низ и у случају да је бинарни тада има сличне карактеристике као и случајни низ. Криптографски кључ се у виду бинарног низа генерише алгоритмом. Неопходно је коришћење алгоритма како би се кључ генерисао и на страни пошиљаоца и

на страни примаоца, и такав алгоритам се назива детерминистички. Псеудослучајни низови су периодични у ширем смислу, па период низа мора бити барем исте дужине као и низ који се шифрује.



Слика 2.1: Схематски приказ секвенцијалног шифрарског система

2.1.2 Блок криптографски системи

Код оваквих алгоритама основна порука која се енкриптује дијели се на блокове фиксне дужине и енкрипција се врши на нивоу блока. Сваки блок шифрује се истим кључем. Дужина блока је најчешће 64 или 128 бита. Шифровање сваког елемента зависи од начина шифровања елемената између којих је позициониран. Дешифровање шифрата се врши од почетка до краја и тако се добија отворени текст. Уколико је неопходно, може се дешифровати само један блок. Основни елементи блок шифрарског система су:

(1) Почетна трансформација

(2) Криптографски слаба функција која се понавља

(3) Коначна трансформација

(4) Алгоритам за развој кључа

Блок шифрарски системи се најчешће користе за шифровање кратких порука, лозинки, криптографских кључева, идентификационих података. Најпознатији блок криптографски системи су BLOWFISH, TWOFISH, DES, AES.

Основни проблеми у оваквим системима су сигурна размјена тајног кључа и немогућност дигиталног потписивања.

2.2 Асиметрични криптографски системи

Темеље асимеричне криптографије поставили су Витфилд Дифи и Едвард Хелман[4] који су заступали идеју да се криптографија заснива на постојању јавног и тајног кључа. Ове алгоритме називамо још и PKI (public-key-algorithms), односно алгоритми са јавним кључем. Оно што је специфично за овај тип алгоритма је да се користе два кључа за енкрипцију и декрипцију основне поруке. Један он њих је јаван и доступан свима, док је други доступан само његовом власнику. Кључеви су у ствари два узајамно проста броја.

Нека је E_{k_1} функција енкрипције кључем k_1 и D_{k_2} функција декрипције кључем k_2. Нека M означава скуп изворних порука, а X скуп шифрованих порука. Процесе енкрипције и декрипције можемо описати на следећи начин:

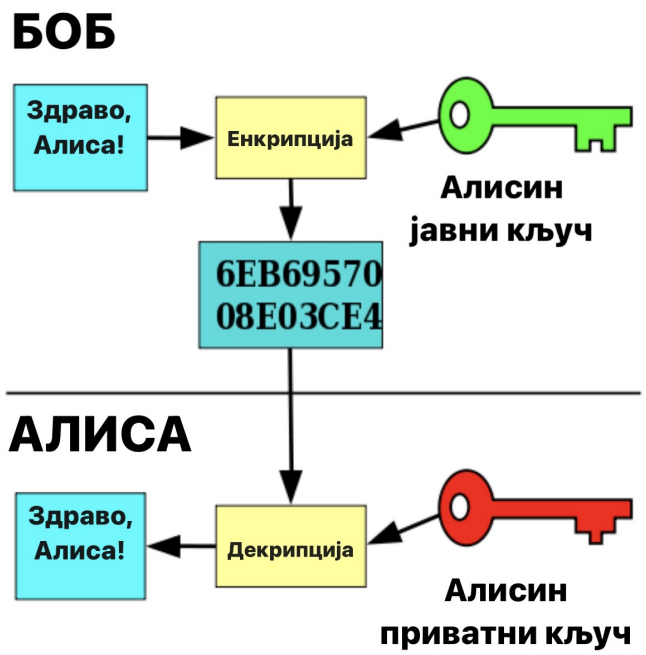
$$E_{k_1} : M \to X$$

$$D_{k_2} : X \to M$$

[4]Bailey Whitfield Diffie и Martin Edward Hellman су познати амерички криптографи, добитници Тјурингове награде

Даље се може примијетити да за сваку изворну поруку m из скупа M важи:

$$D_{k_2}(E_{k_1}(m)) = m$$



Слика 2.2: Сигурна размјена порука без размјене кључа

Овакво шифровање јавним а дешифровање тајним кључем показало се такође као одлично својство и омогућава дигитално потписивање информација гдје се аутентичност може провјерити јавним кључем. Потребно је обезбиједити да се приватни кључ не смије никако израчунати из јавног кључа или барем не у реалном времену. Кључеви требају бити повезани неком једносмјерном функцијом.

Дефиниција 2.2 (One-Way функција)**.** *Функција $f : D \to R$ која има особину да је лако израчунати $f(x)$ за свако $x \in D$ и тешко наћи било какву информацију о x на основу $f(x)$ се назива криптографска one-way (једносмјерна) функција. [2]*

Уколико је позната нека додатна информација о one-way функцији онда се

може пронаћи њена инверзна функција. Додатну информацију називамо замком, а саму функцију (Trapdoor One-Way Function) или функција са замком.

Сам процес комуникације би изгледао овако: уколико учесник A хоће да пошаље поруку m учеснику B неопходно је да пронађе јавни кључ E_b учесника B. Након тога A уз помоћ E_b рачуна функцију f_b и шаље кориснику B поруку $f_b(m) = c$. Искључиво корисник B може да израчуна инверзну функцију ${f_b}^{-1}$ и уз помоћ ње дешифрује оригиналну поруку m.

$$ {f_b}^{-1}(c) = {f_b}^{-1}(f_b(m)) = m $$

Претходно описани процес комуникације је значајан напредак у криптографији, међутим треба имати на уму да не постоји адекватан математички доказ о егзистенцији једносмјерне функције, као и једносмјерне функције са замком. Такође, не постоји ни доказ да не постоји алгоритам за лако израчунавање инверзне функције, али постоје кандидати за које се може рећи да посједују својства једносмјерних функција као што су:

- Производ великих простих бројева, чија је инверзна функција растављање добијеног резултата на просте чиниоце.
- Дискретно степеновање чија је инверзна функција проблем проналажења дискретног логаритма
- Knapsack - проблем тражења тачне суме

Безбједност криптографских система са јавним кључевима зависи од броја операција које је потребно извршити да би се израчунала инверзна функција. Главни недостатак је спорост и неприкладност за шифровање великих количина

података. Често коришћени асиметрични алгоритми су PCA (Rivest-Shamir-Adleman), Дифи-Хелман, ЕлГамал, Рабин, Елиптичне криве.

Глава 3

Елиптичне криве

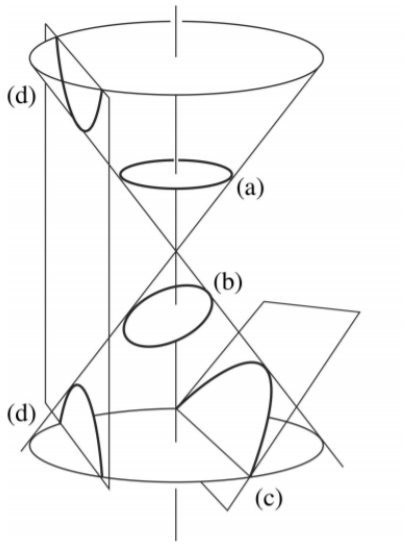
Елиптичне криве представљају фамилију глатких алгебарских кривих, односно могу се описати алгебарским изразом и први извод им је дефинисан у свакој тачки домена у којој је крива дефинисана. У општем, криве представљају скуп неповезаних тачака које задовољавају одређену једначину и немају назив елиптичне због облика елипсе. Елиптичне криве се примјењују у многим областима математике, а њихова примјена у криптографији биће детаљније описана у наставку овог рада.

3.1 Алгебарске криве

Дефиниција 3.1 (Алгебарске криве)**.** *Алгебарске криве представаљају геометријско мјесто тачака у равни које се могу дефинисати алгебарским изразом* $f(x, y) = 0$.

Раван у којој се дефинишу алгебарске криве је дводимензионална Еуклидова раван. Ред алгебарске криве одређује највећи степен у полиному. Степен алгебарског израза који дефинише конусни пресјек одређује ред алгебарске криве која настаје у пресјеку. Фамилија алгебарских кривих другог реда је најчешће

проучавана и употребљавана, а њени представници су конусни или Аполонијеви[1] пресјеци. Конусни пресјеци настају сјечењем неке равни са два идентична конуса спојена врховима.



Слика 3.1: a) круг, b) елипса, c) парабола, d) хипербола [3]

Алгебарске криве трећег степена се јављају у више облика од којих је најједноставнији:

$$y^2 = ax^3 + bx^2 + cx + d, \quad a \neq 0 \tag{3.1.1}$$

Елиптичне криве спадају у фамилију алгебарских кривих трећег степена.

[1]Аполоније из Пергама (грч. *Apollonii Pergaei*; 262 п. н. е. - 190 п. н. е.) је антички математичар и астроном, познати научник александријског Музеона називан још и „Велики геометар".

3.2 Дефинисање елиптичне криве

Дефиниција 3.2 (Елиптичне криве)**.** *Елиптичне криве представљају геометријско мјесто тачака у равни чији је положај дефинисан алгебарским изразом:*

$$y^2 = x^3 + ax + b\,, \quad a, b \in \mathbb{R} \tag{3.2.1}$$

Претходно наведени израз представља Вајерштрасову[2] нормалну форму елиптичних кривих. Елиптична крива је заправо глатка несингуларна крива са тачком O која означава бесконачност. Геометријски, несингуларност значи да нема самопресијецања ни у једној тачки, да нема изолованих тачака и да нема „шиљака".

У једначини (3.2.1) a и b су карактеристични коефицијенти једначине који одређују које тачке ће бити на кривој.

$$\Delta = -16(4a^3 + 27b^2) \tag{3.2.2}$$

Израз (3.2.2) се назива дискриминанта једначине. Да би крива задовољила услов несингуларности, односно регуларности дискриминанта мора бити различита од нуле. Еквивалентно са тим, важи и да су коријени полинома $x^3 + ax + b$ различити што слиједи из:

$$(x, y) = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0 \tag{3.2.3}$$

[2]Карл Вајерштрас (1815-1897) - њемачки математичар и професор Универзитета у Берлину

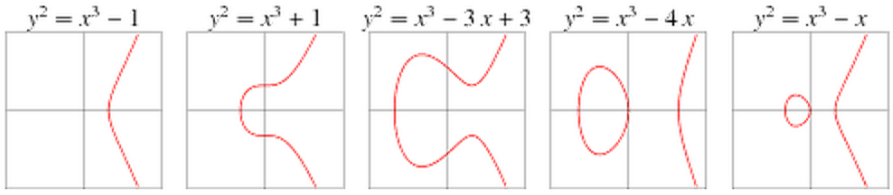
Нека је E скуп тачака елиптичне криве којима је придружена тачка O са координатама $(-\infty, +\infty)$, односно:

$$E = \{(x, y) \mid y^2 = x^3 + ax + b\} \cup \{O\} \tag{3.2.4}$$

Уз помоћ неких геометријских својстава може се показати да тачке скупа E формирају Абелову групу у односу на сабирање, што ће бити показано у наредним поглављима.

3.3 Геометријска интерпретација

Посматрајући израз (3.2.1) увиђа се да се елиптична крива може изразити као квадратна зависност y-координате од трећег степена x-координате. У зависности од параметара a и b график елиптичне криве изгледа различито што се може видјети на слици 3.2.



Слика 3.2: Неки карактеристични графици елиптичних кривих [4]

3.4 Коначна поља

Поље је алгебарска структура над чијим елементима су дефинисане операције сабирања, одузимања, множења и дијељења (осим нулом) за које важе основна аритметичка правила.

Дефиниција 3.3 (Поље)**.** *Непразан скуп* $\big(R,+,\cdot\big)$ *назива се поље уколико за операције* $+$ *и* $\cdot$ *важе следећи услови:*

(1) $\big(R,+\big)$ *је Абелова група.*

(2) $\big(R,\cdot\big)$ *је Абелова група.*

(3) $\forall a,b,c \in R\ a\cdot(b+c) = a\cdot b + a\cdot c$ *важи* ***дистрибутивност*** *множења према сабирању.*

Елиптичне криве које се примјењују у криптографији се посматрају над коначним пољима $\mathbb{F}_p$ и $\mathbb{F}_{2^m}$. **Коначна поља** су поља са коначним бројем елемената.

3.4.1 Коначно поље $\mathbb{Z}_p$

Коначно поље $\mathbb{Z}_p$, гдје је p прост број или $p = q^m$ за $m \in \mathbb{N}$ и q прост број, садржи p елемената који се могу представити као скуп цијелих бројева:

$$\{0,1,2,...,p-1\} \tag{3.4.1}$$

За сваки прост број p постоји јединствено коначно поље $\mathbb{F}_p$. На пољу $\mathbb{F}_p$ могу се дефинисати следеће операције:

- сабирање по модулу p дефинисано тако да $\big(\forall a,b \in \mathbb{F}_p\big)\ a+b = r$, гдје је $r \in \{0,1,2,...,p-1\}$ остатак при дијељењу збира $a+b$ са p
- множење по модулу p дефинисано тако да $\big(\forall a,b \in \mathbb{F}_p\big)\ a\cdot b = m$, гдје је $m \in \{0,1,2,...,p-1\}$ остатак при дијељењу производа $a\cdot b$ са p

Неутрални елемент у односу на сабирање је $0 \in \mathbb{F}_p$, а инверзни елемент за $a \in \mathbb{F}_p$ је елемент $-a \in \mathbb{F}_p$ који је јединствено рјешење једначине $a + x \equiv 0 \pmod{p}$. За

операцију множења неутрални елемент је $1 \in \mathbb{F}_p$, а инверзни елемент за $a \in \mathbb{F}_p$, $a \neq 0$ је елемент $a^{-1} \in \mathbb{F}_p$ који је јединствено рјешење једначине $a \cdot x \equiv 1 \pmod{p}$. Наведене једначине задовољавају услове из дефиниције 3.3.

3.4.2 Коначно поље $\mathbb{Z}_{2^m}$

Посматрајмо коначно поље $\mathbb{F}_p$ и $p = q^m$ гдје је m природан, а q прост број. Може се закључити да постоји јединствено (до на изоморфизам) поље $\mathbb{F}_p$, чија је једна од реализација $\mathbb{Z}_q/f(x)$, гдје је $f(x)$ неразложив полином степена m. Елементи овако заданог поља су полиноми над пољем $\mathbb{Z}_q$ степена мањег или једнаког од $m-1$. Операције сабирања и дијељења у оваквом пољу се наслеђују из $\mathbb{Z}_q$, с тим што се на добијени резултат рачуна остатак при дијељењу са полиномом $f(x)$. Показује се да је најпогодније изабрати полином $f(x)$ са што мање ненултих коефицијената да би операције из поља $\mathbb{F}_p$ биле погодније за примјену над елитпичним кривим.

Коначно поље $\mathbb{F}_{2^m}$ има 2^m елемената које можемо представити као скуп бинарних полинома степена мањег или једнаког $m-1$:

$$\{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + ... + a_1x^1 + a_0 : a_i \in \{0,1\}\} \tag{3.4.2}$$

Операције сабирања и одузимања су дефинисане као у пољу $\mathbb{Z}_p$.

3.5 Аритметика над тачкама елиптичне криве

Као битна својства елиптичних кривих могу се издвојити следећа тврђења:

- За двије различите тачке на елиптичној кривој може се увијек јединствено описати трећа тачка која је пресјек криве и праве кроз те двије тачке.

- У случају да је права тангента на криву у некој тачки, онда се та тачка броји два пута.

- Тачно један од ових услова важи за било који пар тачака на елиптичној кривој. [4]

Користећи ова својства можемо дефинисати операције сабирања различитих тачака на кривој и сабирање тачке са самом собом.

3.5.1 Сабирање двије различите тачке елиптичне криве

Нека су P и Q двије различите тачке скупа E дефинисаног изразом (3.2.4) које припадају графику елиптичне криве. Кроз двије тачке у равни може се повући једна и само једна права. Нека је права l сјечица графика која пролази кроз тачке P и Q. Коефицијент правца праве l се може израчунати као тангенс угла који права l заклапа са позитивним дијелом x-осе. Ако тачке P и Q имају координате (x_1, y_1) и (x_2, y_2) тада се k рачуна:

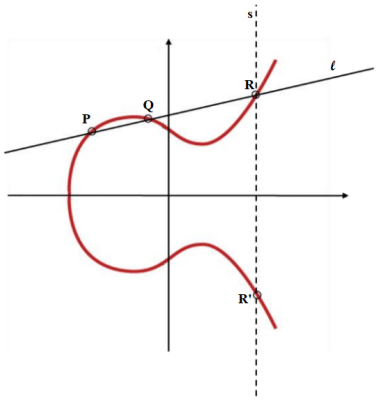
$$k = \tan\alpha = \frac{y_2 - y_1}{x_2 - x_1} \tag{3.5.1}$$

На основу претходно наведених својстава може се рећи да права l пресијеца криву у још једној, трећој тачки. Означимо је са R. Сабирање тачака P и Q дефинише се као осна симетрија кроз x-осу треће тачке пресјека на линији која пролази кроз P и Q.

Нека је сада, s права која пролази кроз тачку R и паралелна је са y-осом, што значи да је истовремено нормална на x-осу. У другом пресјеку праве s и графика криве налази се тачка, у ознаци R', која је осно симетрична тачки R у односу на x-осу правоуглог координатног система. Тачка R' представља резултат сабирања

тачака P и Q.

Описани поступак може се графички интерпретирати сликом 3.3.



Слика 3.3: Графички приказ сабирања двије различите тачке на елиптичној кривој [5]

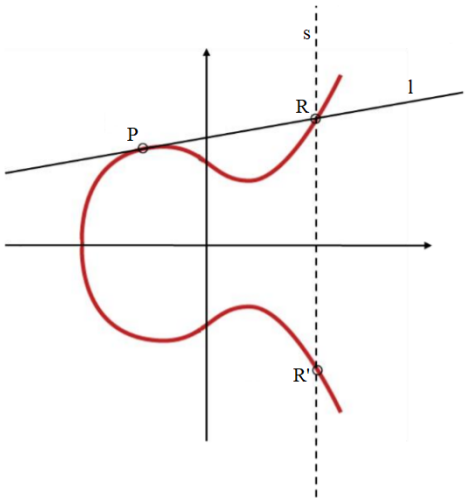
3.5.2 Сабирање тачке елиптичне криве са самом собом

За сабирање тачке P са самом собом потребно је поставити тангенту на криву у тачки P. Посматрајући израз (3.5.1) може се закључити да тачка Q тежи дуж криве ка тачки P када $x_2 \to x_1$. Истовремено, коефицијент правца сјечице тежи коефицијенту правца тангенте, па имамо:

$$k = \tan\alpha = \lim_{x_2 \to x_1} \frac{y_2 - y_1}{x_2 - x_1} \tag{3.5.2}$$

Нека је l тангента на криву у тачки P и R тачка пресјека тангенте и криве. Даље, нека је s права која пролази кроз тачку R, паралелна са y-осом односно нормална на x-осу. Пресјек праве s и графика криве образује тачку R' која је осно симетрична тачки R у односу на x-осу. Тачка R' представља сабирање тачке P са самом собом.

Претходно описани поступак може се графички интерпретирати сликом 3.4.



Слика 3.4: Графички приказ сабирања тачке елиптичне криве са самом собом [5]

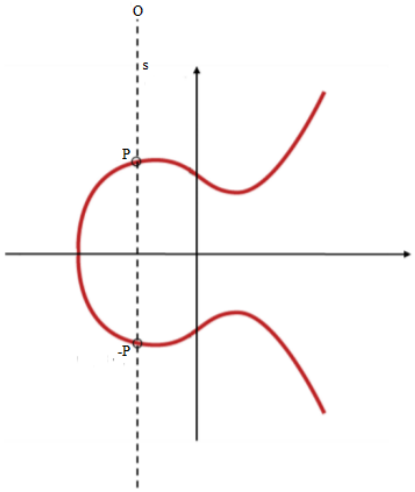
Из претходног је јасно да се може извршити и вишеструко сабирање тачке са елиптичне криве. За $n-$тоструко сабирање умјесто n узастопних сабирања ефикасније је користити што више дуплираних сабирака. Уколико говоримо о $n-$тоструком сабирању имамо два случаја:

- n-парно: $nP = P + P... + P = 2P + 2P... + 2P = 2\left(\frac{n}{2}P\right)$
- n-непарно: $nP = P + P + ... + P = 2P... + 2P + P = 2(n-1)P + P$

3.5.3 Налажење супротног елемента на скупу

Нека је P тачка са графика елиптичне криве. Повлачећи кроз тачку P праву s паралелну са y-осом, односно нормалну на x-осу, у пресјеку са графиком криве добија се тачка $-P$ која је осно симетрична тачки P у односу на x-осу. За сабирање тачака P и $-P$ неопходно је наћи трећу тачку пресјека са графиком криве која у овом случају не постоји. Тачка O из дефиниције скупа E налази се у бесконачности и дефинише се правило да тачка O припада било којој правој која

је паралелна y-оси, односно било којој вертикали. Дакле, тачка O представља резултат сабирања тачака P и $-P$, односно неутрални елемент, док тачка $-P$ представља супротни елемент тачки P на скупу E.



Слика 3.5: Графички приказ одређивања супротног елемента [5]

3.6 Алгебра елиптичних кривих

У оквиру алгебарске интерпретације операција над скупом E, задатог изразом (3.2.4) потребно је увести појам Абелове групе као и показати њену егзистенцију над скупом E у односу на операцију сабирања.

Дефиниција 3.4 (Абелова група)**.** *Непразан скуп S заједно са бинарном операцијом „$*$" која је дефинисана на S, у ознаци $(S, *)$, назива се Абелова група ако важе следећи услови:*

(1) *ако $x, y \in S$ тада $x * y \in S$ (**затвореност**)*

(2) $(\forall x, y, z \in S)$ $x * (y * z) = (x * y) * z$ *(**асоцијативност**)*

(3) $\big(\exists e \in S\big)\big(\forall x \in S\big)\ x * e = e * x = x$ *(**неутрални елемент**)*

(4) $\big(\forall x \in S\big)\big(\exists x' \in S\big)\ x * x' = x' * x = e$ *(**инверзни елемент**)*

(5) $\big(\forall x, y \in S\big)\ x * y = y * x$ *(**комутативност**)*

3.6.1 Абелова група на скупу E

Нека су P i Q двије различите тачке скупа E задатог изразом (3.2.4) и нека имају координате $P(x_1, y_1)$ i $Q(x_2, y_2)$. Нека је права l која повезује тачке P и Q задата једначином:

$$l : y = \lambda x + n \tag{3.6.1}$$

гдје је λ коефицијент правца праве, а n представља одсјечак праве на y-оси. Како се ради о елиптичним кривим, λ и n се израчунавају по формули:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, P \neq Q \\ \frac{3{x_1}^2 - a}{2y_1}, P = Q \end{cases} \qquad \text{i} \qquad n = y_1 - \lambda x_1$$

Пресјечне тачке праве l и елиптичне криве се рачунају по формули:

$$(\lambda x_1 + n)^2 = x^3 + ax + b \tag{3.6.2}$$

Претходна једначина има три рјешења од којих су два тачке P и Q, јер задовољавају и једначину криве и једначину праве l. Треће рјешење једначине (3.6.2) гласи:

$$x_3 = \lambda^2 - x_1 - x_2 \qquad \wedge \qquad y_3 = \lambda x_3 + n$$

Важно је напоменути да се на скупу E могу дефинисати следећа правила при сабирању тачака:

(1) Ако је $P \neq Q$ и $x_1 = x_2$ тада је $P + Q = O$

(2) Ако је $P = Q$ и $y_1 = 0$ тада је $P + Q = 2P = O$

(3) Ако је $P \neq Q$ и $x_1 \neq x_2$ тада је $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ и $n = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$

(4) Ако је $P = Q$ и $y_1 \neq 0$ тада је $\lambda = \frac{3{x_1}^2 + a}{2y_1}$ и $n = \frac{-x^3 + ax + 2b}{2y}$ [5]

Имајући у виду задато правило сабирања у потпоглављу 3.5.1 добија се:

$$P + Q = (x_3, -y_3) \tag{3.6.3}$$

Односно,

$$P + Q = (\lambda^2 - x_1 - x_2, \lambda^3 + \lambda(x_1 + x_2) - n) \tag{3.6.4}$$

Из претходног се може закључити да на скупу E важе услови затворености, услови постојања инверзног и неутралног елемента. Такође, лако се може провјерити да важе услови асоцијативности и комутативности.

У коначном, скуп E чини Абелову групу у односу на операцију дефинисану на претходно описани начин. Односно, може се дефинисати операција која тачке елиптичне криве преводи у Абелову групу.

Нека додатна својства елиптичних кривих биће објашњена у даљем тексту гдје ће бити обрађене неке примјене елиптичних кривих у криптографији.

Глава 4

Елиптичне криве и ДЛОГ проблем

Криптографија елиптичних кривих (ECC - *Elliptic Curve Cryptography*) настала је као алтернатива за постојеће имплементације криптографије са јавним кључем. Базирана је на елиптичним кривим над коначним пољима.

4.1 ДЛОГ проблем у коначном пољу

Сигурност криптосистема са јавним кључем се заснива на тешкоћи налажења дискретног логаритма. Идеја се састоји у томе да је тешко из функције енкрипције, у реалном времену, наћи неки податак о функцији декрипције.

Дефиниција 4.1 (Циклична група)**.** *За групу* $(G, *)$ *кажемо да је* ***циклична*** *ако постоји елемент* $g \in G$ *тако да за свако* $h \in G$ *важи* $h = \underbrace{g * g * ... * g}_{k}$ *односно* $G =< g >$*. Елемент* g *је* ***генератор*** *групе* G*.*

За увођење појма дискретног логаритма потребно је дефинисати коначну Абелову групу тако да су операције множења и степеновања на њој једноставне, док логаритмовање, као инверзна операција операцији степеновања, треба бити доста тешко. У криптографији се најчешће користи циклична, мултипликативна група $\mathbb{Z}_p^*$ као скуп свих остатака при дијељењу са простим бројем p. Генератор групе $\mathbb{Z}_p^*$

назива се **примитивни коријен** по модулу p. Број $g \in \{0, 1, 2, ..., p-1\}$ се назива примитивни коријен по модулу p ако је $p-1$ најмањи степен броја g који даје остатак 1 при дијељењу са p. Најмањи цијели број x тако да је $g \cdot x \equiv 1 \pmod{p}$ назива се мултипликативни инверз од g по модулу p.[6]

Дефиниција 4.2 (Дискретни логаритам)**.** *Нека је g генератор цикличне групе $\mathbb{Z}_p^*$ и h произвољан, ненулти елемент групе. Проблем дискретног логаритма је проблем налажења експонента x тако да*

$$g^x \equiv h \pmod{p}$$

Број x називамо дискретним логаритмом од h у односу на базу g и означавамо га $\log_g(h)$. [2]

Проблем дискретног логаритма се сматра једном врстом једносмјерне функције и можемо га проширити на уопштену цикличну групу. Чињеница да постоје групе у којима је проблем дискретног логаритма тежак представља један од рјешења проблема размјене кључева. Алгоритми за рјешавање проблема дискретног логаритма могу се сврстати у три категорије:

- Алгоритми који раде у произвољним групама као што су: метод грубе силе (brute force), Шанксов алгоритам, Полард-ро.
- Алгоритми који раде у групама чији ред нема велике просте факторе као што је Полиг-Хелман алгоритам.
- Алгоритми који се заснивају на методама представљања елемената групе као производа елемената из релативно малих скупова, такозваних факторских база. Класични представници ове категорије су алгоритми који су варијације индекс калкулус методе.

Примјер 4.1 (ДЛОГ). *Тражимо дискретни логаритам у пољу* $\mathbb{Z}_{47}$ *од* 41 *по основи* 5. *Знамо да је* 5 *генератор мултипликативне групе. Метод грубе силе (brute force attack) нам даје рјешење конгруенције:*

$$5^x \equiv 41 \pmod{47}$$

за $x = 15$. *Није лако користећи просто претраживање наћи дискретни логаритам, чак и за неке простије примјере. [2]*

4.2 ДЛОГ проблем са елиптичним кривим

Размотримо сада појам дискретног логаритма заснованог на елиптичним кривим (ECDLP - Elliptic Curve Discrete Logarithm Problem). Налазимо се у коначном пољу и битан параметар је број тачака елиптичне криве над изабраним пољем. Кроз примјере ћемо показати како одредити групу $E(\mathbb{F}_p)$ уз коришћење нешто мањих вриједности броја p као и одредити број елемената у њој. За $p \neq 2$ пола елемената су квадрати.

Примјер 4.2. *У пољу* $\mathbb{F}_{13}$ *имамо квадрате:* $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 3$, $5^2 = 12$, $6^2 = 10$, $7^2 = 10$, $8^2 = 12$, $9^2 = 3$, $10^2 = 9$, $11^2 = 4$, $12^2 = 1$. *Једначина* $y^2 = 12$ *има два рјешења* $y = 5 \wedge y = -5$, *односно* $y = 5 \wedge y = 8$. *Ако је* g *генератор, онда су* g^{2k} *квадрати, а* g^{2k-1} *нису. [7]*

Постоје ефикасни алгоритми за утврђивање да ли је неки елемент поља квадтат и за рачунање коријена из њега, ако јесте.

Примјер 4.3. *Нека је* E *крива* $y^2 = x^3 + 1$. *Одредити* $E(\mathbb{F}_5)$ *(наћи тачке са координатама у* $\mathbb{F}_5$ *и одредити број елемената)*
Прво ћемо израчунати квадрате: $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, $4^2 = 1$.

x	x^3+1	$y=\pm\sqrt{x^3+1}$	*тачке*
0	1	$\pm 1 = 1, 4$	$(0,1),(0,4)$
1	2		
2	4	$\pm 2 = 2, 3$	$(2,2),(2,3)$
3	3		
4	0	0	$(4,0)$
			$\emptyset$

Из табеле видимо да скуп $E(\mathbb{F}_5)$ *има* 6 *тачака. Тачке над коначним пољем могу се сабирати коришћењем једначина правих или примјеном израза за сабирање. Ако је* $G=(2,3)$ *онда је* $2G=(0,1)$, $3G=(4,0)$ $4G=(0,4)$ *(примјећујемо да ова тачка има исту* x*-координату као и* $2G$ *па је* $4G=-2G$ *),* $5G=(2,2)$, $6G=\emptyset$. *Видимо да је* $G=(2,3)$ *генератор групе* $E(\mathbb{F}_5)$. *[7]*

Примјер 4.4. *Нека је* E *крива* $y^2=x^3+x+1$ *над пољем* $\mathbb{F}_{109}$. *Испоставља се да је скуп* $E(\mathbb{F}_{109})$ *има* 123 *тачке као и да је генерисан тачком* $G=(0,1)$. *Тачка* $(39,45)$ *је у* $E(\mathbb{F}_{109})$ *јер* $39^2+39+1\equiv 63 \pmod{109}$ *и* $45^2\equiv 63 \pmod{109}$. *Дакле,* $(39,45)=(0,1)+(0,1)+...+(0,1)=n(0,1)$ *за неки природан број* n. *[7]*

Одређивање броја n је заправо ДЛОГ проблем са елиптичним кривим над коначним пољима. Проблем се може рјешавати грубом силом, али не и ако се број 109 замијени са простим бројем $\approx 10^{50}$. Овај проблем је тренутно теже ријешити него ДЛОГ проблем, па се могу користити краћи кључеви. Друга предност је та што се за фиксирано коначно поље може посматрати више елиптичних кривих. [7]

4.3 Криптографски системи са елиптичним кривим

Замислимо сада криптографски сценарио по којем особе Алиса и Боб желе остварити комуникацију по претходно утврђеним правилима. Нека је Ева особа која прати њихову комуникацију, покушава да дође до основних порука, као и да промијени њихово значење али и да дође до криптографског кључа што никако не би смјела. У циљу креирања криптосистема базираног на ДЛОГ проблему у пољу $\mathbb{F}_p^*$ кажемо да Алиса објављује два броја g и h. Њен тајни податак је експонент x који је рјешење конгуенције:

$$g^x \equiv h \pmod{p}$$

Алиса може урадити нешто слично и са елиптичном кривом E над $\mathbb{F}_p$. Ако Алиса посматра g и h као елементе групе $\mathbb{F}_p^*$ тада се ДЛОГ проблем своди на налажење x тако да:

$$h \equiv \underbrace{g \cdot g \cdot ... \cdot g}_{x} \pmod{p} \tag{4.3.1}$$

Другим ријечима, да би нашла вриједност x Ева мора да сазна колико пута g треба бити помножено са самим собом да би се добило x тако да задовољава конгруенцију (4.3.1).

Сада је јасно да Алиса може да уради исту ствар и са тачкама које припадају групи $E(\mathbb{F}_p)$ (елиптичној кривој над коначним пољем). Она из скупа $E(\mathbb{F}_p)$ бира и објављује двије тачке P и Q. Њен тајни податак сада је n тако да је:

$$Q = \underbrace{P + P + ... + P}_{n} = nP \tag{4.3.2}$$

Ева сада треба да сазна колико пута је потребно тачку P сабрати са самом собом да би се добила тачка Q. Проблем налажења цијелог броја n се назива **проблем дискретног логаритма за елиптичне криве**. Имајући у виду да је закон сабирања на $E(\mathbb{F}_p)$ веома компликован, теже је доћи до рјешења овако дефинисаног дискретног логаритма.

Дефиниција 4.3. *Нека је E елиптична крива над пољем $\mathbb{F}_p$. ECDLP (*Elliptic Curve Discrete Logarithm Problem*) је проблем налажења цијелог броја n тако да је $Q = nP$. Означава се са $n = \log_P(Q)$ и називамо га **елиптични дискретни логаритам** од Q за базу P.*

Важно је напоменути да уколико Q није вишеструко сабирање тачке P тада логаритам није дефинисан.

4.4 Дифи-Хелман протокол и елиптична размјена кључева

Алиса и Боб желе да остваре комуникацију неким несигурним комуникационим каналом. Претходно се договарају о избору елиптичне криве $E(\mathbb{F}_p)$ и тачке $P \in E(\mathbb{F}_p)$. Алиса бира скривени податак k_A, док Боб бира скривени податак k_B. Затим обоје самостално рачунају:

$$Q_A = k_A P \qquad \text{i} \qquad Q_B = k_B P$$

и размјењују вриједности Q_A i Q_B.
Алиса и Боб сада користе своје тајне податке и рачунају $k_A Q_B$ и $k_B Q_A$ респективно. Сада обоје посједују исту скривену дијељену вриједност:

$$k_A Q_B = (k_A k_B)P = k_B Q_A = Q_{AB} \tag{4.4.1}$$

Примијетимо да Ева током комуникације може доћи до вриједности $E(\mathbb{F}_p)$, P, Q_A, Q_B. Док вриједности k_A и k_B као и вриједност Q_{AB} која јој је потребна за напад остају непознати за Еву. Да би дошла до тајне вриједности Ева мора да ријеши проблем дискретног логаритма за елиптичне криве како би из Q_A дошла до k_A или из Q_B дошла до k_B.

Закључујемо да вриједност из израза (4.4.1) представља тајни податак који посједују обоје и могу га користити као приватни кључ за сигурну комуникацију.

Дефиниција 4.4. *Нека је $E(\mathbb{F}_p)$ елиптична крива над коначним пољем и тачка $P \in E(\mathbb{F}_p)$. ECDH (Elliptic Curve Diffie-Hellman Problem) представља проблем налажења скривене вриједности k_Ak_BP из познатих вриједности k_AP и k_BP. [8]*

Сигурност ECDH протокола зависи од тежине налажења дискретног логаритма за елиптичне криве. У претходно описаном протоколу кључ је број, док Алиса и Боб бирају тачку са елиптичне криве и користе је у поступку. На крају опет добијају тачку Q_{AB} са елиптичне криве. Да би од ње добили број који би им послужио као заједнички кључ трансформишу је у стринг битова.

Посматрајмо тачку $Q_{AB} \in E(\mathbb{F}_p)$ са координатама (x_Q, y_Q), $x_Q, y_Q \in \mathbb{F}_p$. Координате тачке Q_{AB} повезане су формулом:

$$y_Q^2 = x_Q^3 + Ax_Q + B$$

Ева зна коефицијенте A и B, па уколико би некако дошла до вриједности x_Q тада би израчунала двије могуће вриједности за y_Q. С тога, Алиса шаље само x-координату тачке Q_A. Боб рачуна y-координату која има двије могуће вриједности и у зависности од тога добија Q_A или $-Q_A$. У сваком случају, на крају

рачунања Боб добија:

$$\pm k_B Q_A = \pm k_B k_A P$$

Исту вриједност на крају рачунања добија и Алиса. Алиса и Боб су зато у могућности да користе x-координату као заједнички тајни податак јер је x-координата иста без обзира коју су вриједност користили за y-координату.

4.5 Ел Гамал и елиптичне криве

Један од најзначајнијих криптографских система који се заснивају на Дифи-Хелман протоколу је Ел Гамал криптосистем. Опет замислимо криптографски сценарио у којем Алиса и Боб желе да изврше сигурну размјену порука. Прво се договарају о избору елиптичне криве $E \in E(\mathbb{F}_p)$, гдје је p прост број. Алиса жели да пошаље Бобу поруку. Боб бира скривени број k_B и објављује свој јавни кључ $Q_B = k_B P$. Алисина порука је заправо тачка $M \in E(\mathbb{F}_p)$. Она бира свој привремени кључ, а затим рачуна:

$$C_1 = kP \qquad \text{i} \qquad C_2 = M + kQ_B \tag{4.5.1}$$

Алиса шаље уређени пар (C_1, C_2) Бобу који затим, да би открио изворну поруку, рачуна:

$$C_2 - k_B C_1 = (M + kQ_B) - k_B(kP) = M + k(k_B P) - k_B(kP) = M [8] \tag{4.5.2}$$

У принципу, Ел Гамал алгоритам ради добро, али у пракси постоје неки недостаци. Први недостатак је како кодирати поруку као тачку што ће бити објашњено у следећем примјеру.

Примјер 4.5. *За конструкцију поља* $\mathbb{F}_p$ *узмимо прост број* $p = 257$*. Замислимо ситуацију да свако слово има свој редни број у пољу. Најједноставније би било кодирати тај број* x*-координатом неке тачке али нису сви бројеви* x*-координате неких тачака, што важи и за* y*-координате. Умјесто тога, нека број који се добија дописивањем једне цифре редном броју слова служи као код тог слова. Пошто имамо* 10 *цифара на располагању, а свака од њих даје потенцијалну* x*-координату са вјероватноћом* 50%*. Поруци се, у пракси, може додати* 8 *бита, тако да је вјероватноћа проблема приближно једнака нули.*

Нека су Алиса и Боб изабрали елиптичну криву $E : y^2 = x^3 - 4$*. Алиса жели да пошаље поруку садржине* L *и знамо да је редни број тог слова* 11*. Треба одредити тачку* $(11a, y)$ *на кривој. Како посебан алгоритам не постоји, испробавамо редом бројеве* $110, 111, 112...$

$$x = 110, \quad 110^3 - 4 \equiv 250 \neq k^2 \pmod{257}$$

$$x = 111, \quad 111^3 - 4 \equiv 130 \neq k^2 \pmod{257}$$

$$x = 112, \quad 112^3 - 4 \equiv 250 \equiv k^2 \pmod{257}$$

Дакле, $(112, 26)$ *је тачка на елиптичној кривој тако да су све цифре* x*-координате, осим последње, заправо порука.*

За тачку P *узмимо тачку* $(2, 2)$ *(припада елиптичној кривој јер задовољава једначину* $2^2 = 2^3 - 4$*). Боб је изабрао свој скривени број* $k_B = 101$ *па је Бобов јавни кључ* $k_B P = 101(2, 2) = (197, 167)$*.*

Алиса сада Бобу треба да пошаље тачку $(112, 26)$*, коју означавамо са* Q*. Алиса бира тајни кључ поруке* $k = 41$ *и рачуна:*

$kP = 41(2, 2) = (136, 128)$*,*

$kk_BP = 41(197, 167) = (68, 84)$

$Q + kk_BP = (112, 26) + (68, 84) = (246, 174).$

Алиса шаље пар тачака kP *и* $Q + k(k_BP)$ *односно* $(136, 128)$ *и* $(246, 174)$.

Боб прима пар тачака и да би открио изворну поруку рачуна:

$k_BkP = 101(136, 128) = (68, 84)$ *и тражи тачку* $(Q + kk_BP) - (k_BkP)$*, односно:*

$(246, 174) - (168, 84) = (246, 174) + (68, -84) = (112, 24)$

Боб затим узима све сем последње цифре x*-координате и добија* $11 = L$*.[7]*

4.6 Полард-ро алгоритам напада

За нападе опште намјене најефикасније су примјене Полиг-Хелман и Полард-ро алгоритма. Претпоставимо да постоје различити парови цијелих бројева (c', d') і (c'', d'') по модулу n тако да задовољавају следећи услов:

$$c'P + d'Q = c''P + d''Q \tag{4.6.1}$$

Даље је:

$$(c' - c'')P = (d' - d'')Q = (d' - d'')lP \tag{4.6.2}$$

$$c' - c'' \equiv (d' - d'')l \pmod{n} \tag{4.6.3}$$

Број $l = \log_P Q$ се може израчунати на следећи начин:

$$l \equiv (c' - c'')(d' - d'')^{-1} \pmod{n} \tag{4.6.4}$$

Дефинишимо итеративну функцију $f :< P > \rightarrow < P >$ са:

$$f(X) = X + a_jP + b_jQ \tag{4.6.5}$$

тако да произвољна тачка $X_0 \in < P >$ може образовати низ $\{X_i\}_{i \geq 0}$ за који важи да је $X_i = f(X_{i-1})$, $i \geq 1$. Нека је j индекс одговарајућег пара цијелих бројева дефинисан функцијом $H(X) = j$ и $X = cP + dQ$. Полард-ро напад на ECDLP се може описати на следећи начин:

Улазни параметри су $P \in \mathbb{F}_p$ реда n и $Q \in < P >$, а излазни $\log_P Q$

- Изабере се број L реда 2
- Изабере се функција H са интервала $\{1, 2, ..., L\}$
- За j које се мијења од 1 до L врше се следећа израчунавања:
  - Изабере се $a_j, b_j \in_R [0, n-1]$
  - Израчуна се $R_j = a_j P + b_j Q$
- Изабере се $c', d' \in_R [0, n-1]$ и израчуна се $X' = c'P + d'Q$
- Додијеле се вриједности: $X'' \leftarrow X'$, $c'' \leftarrow c', d'' \leftarrow d'$
- Понавља се следеће израчунавање све док не буде испуњен услов да је $X' = X''$
  - Израчунава се $j = H(X')$

    Додјељују се вриједности $X' \leftarrow X' + R_j$, $c' = c' + a_j \pmod n$, $d' \leftarrow d' + b_j \pmod n$
  - За вриједност i од 1 до 2 врше се следећа израчунавања:

    Израчунава се $j = H(X'')$

    Додјељују се вриједности $X'' \leftarrow X'' + R_j$, $c'' \leftarrow c'' + a_j \pmod n$, $d'' \leftarrow d'' + b_j \pmod n$

    Када је задовољен услов $X' = X''$ израчунавања се завршавају

- Ако је $d' = d''$ алгоритам враћа неуспјех као резултат

  У супротном се израчунава $l = (c' - c'')(d' - d'')^{-1} \pmod{n}$ и као излаз алгоритма се враћа величина l [5]

4.7 Полиг-Хелманов алгоритам напада

Полиг-Хелманом алгоритам чини доста ефикасним рачунање дискретног логаритма $x = \log_P Q$. Нека је дата елиптична крива E над коначним пољем $\mathbb{F}_p$ гдје је тачка $P \in E(\mathbb{F}_p)$ реда n и тачка $Q \in < P >$ (Q припада цикличној групи која је генерисана са P). Ако претпоставимо да n можемо факторисати на r простих чинилаца p_i степенованих са e_i, n можемо записати:

$$n = {p_1}^{e_1} {p_2}^{e_2} ... {p_r}^{e_r} \tag{4.7.1}$$

Полиг-Хелманов алгоритам напада израчунава:

$$x_i \equiv x \pmod{{p_i}^{e_i}}, \quad 1 \leq i \leq r, \;\; x \in [0, n-1] \tag{4.7.2}$$

На тај начин се добија систем конгруентних једначина:

$$x \equiv x_1 \pmod{{p_1}^{e_1}}$$

$$x \equiv x_2 \pmod{{p_2}^{e_2}}$$

$$...$$

$$x \equiv x_r \pmod{{p_r}^{e_r}} \tag{4.7.3}$$

На основу Кинеске теореме о остацима, можемо тврдити да постоји јединствено рјешење система (4.7.3).

Тражено x_i се добија рјешавањем система на следећи начин:

$$x_i = z_0 + z_1 p_i + z_2 {p_i}^2 + ... + z_{e_i-1} {p_i}^{e_i-1} \;\; z \in [0, p_i - 1] \tag{4.7.4}$$

Даље се врши израчунавање:

$$P_0 = \frac{n}{p_i} P \quad Q_0 = \frac{n}{p_i} Q$$

односно,

$$Q_0 = \frac{n}{p_i} Q = \frac{n}{p_i} xP = x\big(\frac{n}{p_i} P\big) = xP_0 = z_0 P_0$$

Из последњег израза се добија тражено z_0:

$$z_0 = \log_{P_0} Q_0$$

На исти начин се добијају остали коефицијенти $z_1, z_2, ..., z_{e-1}$ чиме се добија тражено x_i. [13]

Глава 5

Дигитални потпис примјеном елиптичних кривих

5.1 Дигитални потпис

Дигитални потпис у дигиталном свијету је исто што и својеручни потпис у реалном свијету, односно има исту правну снагу. Његова сврха је провјера идентитета пошиљаоца као и провјера интегритета и непорецивости података. За разлику од својеручног потписа, дигитални потпис је готово немогуће фалсификовати. Потписивање се базира на једној хеш функцији и приватном и јавном кључу. Алгоритам потписивања користи приватни кључ, док алгоритам верификације користи јавни кључ. Проблем се може јавити уколико алгоритам аутентификације траје предуго јер порука може бити произвољне дужине. Важно је напоменути да алгоритам дигиталног потписивања не шифрује податке, већ служи за потврду да подаци нису измијењени.

Дигитални потписи се користе при размјени мултимедијалног садржаја и повјерљивих података у електронском пословању, дистрибуцији софтвера и финансијским трансакцијама. Дигитални потписи су лако преносиви, не могу бити

имитирани, односно не могу се фалсификовати, и могу се означити временском марком.

DSA(Digital Signature Algorithm) представља облик Ел Гамалове схеме дигиталног потписа. То је први облик дигиталног потписа прихваћен од стране владе САД.

Основа сигурности дигиталног потписа је у тајности приватног кључа. Јавни кључ је свима доступан и омогућава провјеру аутентичности поруке. Дигитални потписи се могу користити за све врсте порука, било да су оне кодиране или не. Једноставно прималац поруке може бити сигуран када је у питању идентитиет пошиљаоца, као и у то да је порука стигла непромијењена.

Замислимо да Алиса жели да пошаље Бобу потписану поруку, при чему је e_A Алисин јавни кључ за енкрипцију, а d_A тајни кључ за декрипцију. Процес можемо описати следећим корацима:

- Алиса „дешифрује" основну поруку својим тајним кључем d_A, добија дигитални потпис $S = d_A(M)$ и шаље пар (M, S)
- Боб провјерава да ли је поруку M заиста послала Алиса тако што примјењује Алисин јавни кључ на потпис S:
  $e_A(S) = e_A(d_A(M)) = d_A(e_A(M)) = M$

5.2 Дигитални потпис примјеном елиптичних кривих

Алгоритам дигиталног потписа заснован на елиптичним кривим стандардизован је 1998. године од стране Америчког института за стандардизацију. ECDSA

(Elliptic Curve Digital Signature Algorithm) је варијанта DSA која користи елиптичне криве и њихова својства. Постоје одвојене процедуре за потписивање и аутентификацију и свака се састоји од неколико аритметичких операција. ECDSA се састоји из три корака који ће бити описани у наредним потпоглављима.

5.2.1 Генерисање ECDSA кључева

Процес ћемо посматрати над коначним пољем $\mathbb{F}_p$, гдје је $p = q$, прост број или $p = 2^m$. Радимо са елиптичном кривом $y^2 = x^3 + ax + b$ задатом над пољем $\mathbb{F}_p$ и са ње изаберимо тачку $G(x_g, y_g)$ за коју важи $nG = O$, односно чији је ред n. Претходно наведени подаци су јавни. Генерисање кључева се сада може описати на следећи начин:

- Бира се случајни број d са интервала $[1, n-1]$
- Налази се тачка $Q = dG$ [9]

Јавни кључ је тачка Q док је приватни кључ број d. Важно је напоменути да је потребно провјерити да ли тачка $Q \neq O$ припада изабраној елиптичној кривој, односно да ли задовољава њену једначину као и да ли су њене координате елементи коначног поља $\mathbb{F}_p$. Ред тачке Q такође мора бити n.

5.2.2 Генерисање ECDSA потписа

За потписивање поруке m потребно је начинити следеће кораке:

- Изабрати случајни број $k \in [1, n-1]$
- Израчунати $kG = (x, y)$ и $r \equiv x \pmod{n}$, ако је $r = 0$ поново се бира број k
- Израчунати $t = k^{-1} \pmod{n}$

- Израчунати $e = h(m)$, гдје h представља 160-битну хеш функцију.

- Користећи приватни кључ d израчунати $s \equiv k^{-1}(e + rd) \pmod{n}$, ако је $s = 0$ потребно је вратити се на први корак [9]

Потпис поруке m је уређени пар (r, s)

5.2.3 Верификација

За провјеру потписа (r, s) имамо на располагању јавне параметре p, a, b, G, n, h као и Алисин јавни кључ Q и да би се провјерио потпис морају се испунити следећи кораци:

- Провјерити да ли су r и s бројеви са интервала $[1, n - 1]$

- Израчунати $e = h(m)$

- Израчунати $w = s^{-1} \pmod{n}$

- Израчунати $u_1 = es^{-1} \pmod{n}$ i $u_2 = rs^{-1} \pmod{n}$

- Израчунати тачку $X = (x_1, y_1) = u_1G + u_2Q$

- Уколико је $X = O$ потпис се одбија, иначе се рачуна $v = x_1 \pmod{n}$

- Потпис за поруку m се прихвата ако и само ако је $v = r$. [9]

Примјер 5.1 (ECDSA)**.** *Нека је задата елиптична крива* $y^2 = x^3 + 7$*, (у овом случају имамо* $a = 0, b = 7$*), тачка* $G = (2, 22)$*, поље реда* 79 *и случајно изабрани број* $d = 2$ *који је уједно и приватни кључ. Основна порука која треба да се пошаље је* $m = 17$*.*

Потребно је прво наћи јавни кључ, а како је одабран приватни кључ $d = 2$ *захтијева се само једна операција удвостручавања полазне тачке. Вратимо се*

сада на потпоглавље 3.6.1 *гдје су дате експлицитне формуле за сабирање тачака елиптичних кривих. Како је* $G = Q$, λ *рачунамо по формули* $\lambda = \frac{3x_1^2 - a}{2y_1}$, *односно:*

$\lambda = (3 \cdot 2^2 + 0)/(2 \cdot 22) \pmod{67}$

$\lambda = 12/44 \pmod{67}$

$44^{-1} = 32$

$\lambda = 12 \cdot 32 \pmod{67}$

$\lambda = 384 \pmod{67}$

$\lambda = 49$

Сада координате тражене тачке рачунамо помоћу следећих формула:

$x = \lambda^2 - x_g - x_g$ *i* $y = -(\lambda x + y_g - \lambda x_g)$, *односно:*

$x = (49^2 - 2 - 2) \pmod{67}$

$x = 2397 \pmod{67}$

$x = 52$

$y = -(49 \cdot 52 + 22 - 49 \cdot 2) \pmod{67}$

$y = -2472 \pmod{67}$

$y = 7$

Добили смо јавни кључ $Q(52, 7)$, *док је приватни* 2. *Сада је потребно генерисати потпис следећом процедуром:*

- *Бирање случајног броја*

  $k \in [1, 79 - 1]$

  $k \in [1, 78]$

  $k = 3$

- *Налажење тачке* $kG = (x, y)$ *i* $r \equiv x \pmod{79}$

  $(x, y) = 3G$

$(x, y) = G + 2G$

$(x, y) = (2, 22) + (52, 7)$

$(x, y) = (62, 63)$

$x = 62,\ y = 63$

$r = 62 \pmod{79}$

$r = 62$

- *Налажење* $s = k^{-1}(z + rd) \pmod{79}$

  $s = (17 + 62 \cdot 2)/3 \pmod{79}$

  $s = (17 + 124)/3 \pmod{79}$

  $s = 141/3 \pmod{79}$

  $s = 47 \pmod{79}$

  $s = 47$

Овим смо добили дигитални потпис $(r, s) = (62, 47)$. *Остало је још да извршимо верификацију добијеног дигиталног потписа. Алгоритам се огледа у следећем:*

- *Провјерава да ли* r *и* s *припадају интервалу* $[1, 78]$

  $r = 62 \in [1, 78]$

  $s = 47 \in [1, 78]$

- *Рачунање* $w = s^{-1} \pmod{79}$

  $w = 47^{-1} \pmod{79}$

  $w = 37$

- *Рачунање* $u_1 = zw \pmod{79}$

  $u_1 = 17 \cdot 37 \pmod{79}$

$u_1 = 629 \pmod{79}$

$u_1 = 76$

- *Рачунање* $u_2 = rw \pmod{79}$

$u_2 = 62 \cdot 37 \pmod{79}$

$u_2 = 2294 \pmod{79}$

$u_2 = 3$

- *Налажење тачке* $X = (x, y) = u_1 \cdot G + u_2 \cdot Q$

$u_1 \cdot G = 76 \cdot G$

$u_1 \cdot G = 2 \cdot (38 \cdot G)$

$u_1 \cdot G = 2 \cdot (2 \cdot (19 \cdot G))$

$u_1 \cdot G = 2 \cdot (2 \cdot (G + 18 \cdot G))$

$u_1 \cdot G = 2 \cdot (2 \cdot (G + 2 \cdot (9 \cdot G)))$

$u_1 \cdot G = 2 \cdot (2 \cdot (G + 2 \cdot (G + 8 \cdot G)))$

$u_1 \cdot G = 2 \cdot (2 \cdot (G + 2 \cdot (G + 2 \cdot (4 \cdot G))))$

$u_1 \cdot G = 2 \cdot (2 \cdot (G + 2 \cdot (G + 2 \cdot (2 \cdot (2 \cdot G)))))$

$u_1 \cdot G = 2 \cdot (2 \cdot (G + 2 \cdot (G + 2 \cdot (2 \cdot (2 \cdot (2, 22))))))$

$u_1 \cdot G = 2 \cdot (2 \cdot (G + 2 \cdot (G + 2 \cdot (2 \cdot (52, 7)))))$

$u_1 \cdot G = 2 \cdot (2 \cdot (G + 2 \cdot (G + 2 \cdot (25, 17))))$

$u_1 \cdot G = 2 \cdot (2 \cdot (G + 2 \cdot ((2, 22) + (21, 42))))$

$u_1 \cdot G = 2 \cdot (2 \cdot (G + 2 \cdot (13, 44)))$

$u_1 \cdot G = 2 \cdot (2 \cdot ((2, 22) + (66, 26)))$

$u_1 \cdot G = 2 \cdot (2 \cdot (38, 26))$

$u_1 \cdot G = 2 \cdot (27, 40)$

$u_1 \cdot G = (62, 4)$

Истим поступком рачунамо $u_2 \cdot Q$

$u_2 \cdot Q = 3 \cdot Q$

$u_2 \cdot Q = Q + 2 \cdot Q$

$u_2 \cdot Q = (52, 7) + 2 \cdot (52, 7)$

$u_2 \cdot Q = (52, 7) + (25, 17)$

$u_2 \cdot Q = (11, 20)$

Сада тражено X *рачунамо:* $X = (62, 4) + (11, 20)$

$X = (62, 63)$

- *Остало је још да провјеримо да ли је* $r = x \pmod{79}$

  $62 \equiv 62 \pmod{79}$

  Конгруенција важи па закључујемо да је потпис валидан. [4]

5.3 Сигурност ECDSA

Приликом генерисања ECDSA кључева потребно је одабрати елиптичну криву са неким добрим криптографским особинама. У пракси се најчешће користе неке стандардизоване криве, обично оне које препоручује NIST или Brainpool конзорцијум. [10]

Што се тиче сигурности ECDSA, уколико су параметри који одређују елиптичну криву правилно одабрани, потенцијална опасност је напад на дискретни логаритам над елиптичном кривом. Ако би нападач био у стању да ријеши проблем дискретног логаритма над елиптичним кривим онда би дошао до приватног кључа . Најбољи, до сада познати, напад на криптографију елиптичних кривих има сложеност пропорционалну квадратном коријену величине групе на којој је дефинисан дискретни логатирам. Због тога ECDSA можемо сматрати изузетно сигурним алгоритмом. У следећој табели су приказане битске дужине и нивои сигурности ECDSA. [11]

p	$hesh$ излаз (min)	Нивои сигурности
192	192	96
224	224	112
256	256	128
384	384	192
512	512	256

У алгоритму, ниво сигурности хеш функције мора одговарати нивоу сигурности дискретног логаритма.

Глава 6

Неке савремене примјене елиптичних кривих

Криптосистеми засновани на елиптичним кривим пружају знатно висок степен сигурноси по биту, у односу на неке друге криптографске системе захтијевају много мање меморијских капацитета и много су мање рачунски захтјевни. Због таквих особина веома су погодни за коришћење код малих уређаја са ограниченом меморијом и слабијим процесорима као што су мобилни телефони, паметне картице, електронско пословање итд.

Представу о томе колико је тешко разбити алгоритме који користе криптографију елиптичних кривих у односу на неке стандардне алгоритме дао је Аријен К. Ленстра[1]. Уколико бисмо обим математичких операција потребних за разбијање RSA алгоритма (што није ни мало једноставно) замислили као количину топлоте да се до кључања загрије једна кашичица воде, за разбијање алгоритма елиптичних кривих било би потребно толико топлоте да прокључају сви океани на свијету. Поред тога, постојање одређених недостатака спречава широку употребу оваквих алгоритама. Као једна од осјетљивих ставки издваја се

[1]Arjen Claas Lenstra(1956) је холандски математичар и криптограф, професор на универзитету у Лузијани.

појам „случајности” бројева које је потребно насумично изабрати. Као генератор случајних бројева, једно вријеме се издвајао Dual-EC-DRBG (Dual Elliptic Curve Deterministic Random Bit Generator) којег је стандардизовао NIST(National Institute of Standards and Technology) 2005. године. Међутим, неки од еминентних криптографа, усљед могућности да се предвиде бројеви који се сматрају случајним, га сматрају непоузданим и недовољно заштићеним од потенцијалних напада.

Једна од најпознатијих савремених употреба елиптичних кривих је криптозаштита **Биткоина**. Биткоин је главни представник криптовалута, односно дигиталног, виртуелног новца. Назив Биткоин представља уједно организацију, софтвер и протокол, док биткоин означава јединицу мјере. Биткоин је транспарентан, децентрализован електронски систем трансакција који се не ослања на повјерење већ на сложене криптографске алгоритме. Биткоин користи ECDSA за генерисање дигиталног потписа приликом трансакција. При трансакцијама се не користи изворна порука већ њена хеширана вриједност. За хеширање се користи SHA-256 хеш функција. Поред одређених предности и недостатака, може се рећи да биткоин користи најефикасније методе криптозаштите.

Истовјетан криптографски алгоритам који користи Биткоин, користи и Apple на својим уређајима као што су MacBook, iPad, iPhone. iMessage сервис компаније Apple користи ECC у сврху генерисања дигиталних потписа. И поред великог степена заштите, једна израелска компанија је успјела да разбије криптографски систем који користи Apple. Напад на овакве системе се не ради нападом на сам алгоритам јер би то било бескорисно у односу на расположиве хардверске ресурсе. Умјесто тога, напад се врши на локације гдје се чувају криптографски кључеви и када се једном дође у посјед тајног кључа даље разбијање алгоритма не представља проблем.

Протокол за криптовану размјену информација између сервера и клијента SSL (Security Socket Layer) направљен од стране Netscape компаније 1995. године, првобитно је имао одређене недостатке. С тога се, послије неколико верзија SSL протокола, наметнула потреба настанка TLS (Transport Layer Security) протокола како би се превазишле безбједносне мане првобитно SSL протокола. Док SSL прави експлицитну конекцију путем порта, TLS прави имплицитну конекцију путем протокола. TLS представља темељ данашње сигурне комуникације на интернету. Свака конекција (handshake) заснована је на одређеном алгоритму, односно пакету или сету шифара (chipher suit). При комуникацији између сервера и клијента кључ се генерише помоћу Дифи-Хелман протокола за размјену кључа и ECDH верзија овог протокола је један од најсигурнијих начина за то. У наставку комуникације користи се симетрично шифровање над подацима који се размјењују. Сав саобраћај се шифрује симетричним кључем који је договорен претходно помоћу ECDH протокола. Симетрично шифровање се користи због веће брзине у односу на асиметрично.

Потреба за креирањем безбједног канала преко незаштићене мреже произвела је настанак безбједне верзије протокола за размјену хипертекста HTTPS (HyperText Transfer Protocol Secure) који је комбинација HTTP и SSL/TLS протокола која обезбјеђује енкрипцију и сигурну идентификацију сервера. Уколико се приступа HTTPS верзији Cloudflare блога из неке од новијих верзија претраживача Chrome или Firefox, претраживач ће користити ECC. У Chrome претраживачу се може видјети који криптографски алгоритми се користе за успостављање сигурне конекције кликом на иконицу катанца, који се налази одмах поред адресе сајта који се посјећује. У случају Cloudflare блога добиће се информација да претраживач користи ECDHE (Elliptic Curve Diffie-Helman Ephemeral) протокол. [5]

Криптографске медоте које се користе ради заштите бежичних мрежа подразумијевају, између осталих и протокол који је заснован на елиптичним кривим. TinyECC представља софтверски пакет заснован на елиптичним кривим, који се извршава са циљем успостављања безбједног окружења у бежичној сензорској мрежи.

Можемо закључити да ECC постаје све прикладније рјешење за безбједност и приватност на мрежи.

Глава 7

Закључак

Живимо у времену у којем Интернет има престижну улогу у комуникацији. Широка доступност информација на Интернету има своје предности и мане. Како се Интернетом преносе велике количине података између појединаца, организација или установа самим тим постоји велика опасност по њихову безбједност. Зато је важно заштити их од крађе, неовлашћеног приступа и неовлашћене промјене.

У раду су представљени неки од протокола који су неопходни за правилно и безбједно функционисање Интернета. Криптосистеми који су засновани на елиптичним кривим осигуравају висок степен заштите и при томе штеде на меморијским капацитетима. ECC нуди највиши степен сигурности по биту од свих до сада познатих криптосистема. Брже рачунање у односу на неке стандардне алгоритме уз минималне дужине кључа пружа велику предност криптосистемима заснованим на елиптичним кривим. Видјели смо да је DLP у скупу тачака елиптичне криве прилично тежи за рјешавање од проблема дискретног логаритма над неким другим скуповима. У погледу рјешавања ECDLP није било значајнијих помака у последњих 20 година, док се рјешавање DLP стално усавршава. Уз квалитетан избор случајних параметара избјегава се напад грубом

силом, те је неопходан за правилно и сигурно функционисање алгоритма. Такође, постоје одређене методе за идентификацију учесника у комуникацији.

Иако се константно имплементирају нове верзије за заштиту модерних начина комуникације и чувања података, ECC са својим предностима постаје све прикладније рјешење за очување приватности и безбједности на мрежи.

Библиографија

[1] др Владимир Божовић, *Низ крипто-системи*

[2] др Владимир Божовић, *Увод у асиметричну криптографију-ДЛОГ проблем*

[3] Драгана Чуровић, *Неке познате раванске криве*, мастер рад, Универзитет у Новом Саду, 2015.

[4] Јелена Игњатовић, *Криптографске основе биткоина и електронског банкарства*, мастер рад, Универзитет у Нишу, 2018.

[5] Кристина Куњадић Ћулибрк, *Кипторафија елиптичних кривих*, мастер рад, Универзитет Сингидунум, Београд, 2016.

[6] Теа Схафар, *Криптографија јавног кључа*, Осијек, 2018.

[7] Миодраг Живковић, *Криптографија*, 2020.

[8] J. Hoffstein, J. Pipher, J. Silverman, *An Introduction to Mathematical Cryptography*, untergraduate text in mathematics

[9] Влатка Кривачић, *Криптирање елиптичним кривуљама*, семинарски рад, Загреб, 2004.

[10] D.Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography* Springer-Verlak, New York, 2004.

[11] Даринка Вучинић, *Дигитални потпис*, дипломски рад, Подгорица, 2010.

[12] Sonali Chandel, *A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption*

[13] Darrel Hankerson, Alfred Menezes, Scott Vanstone, *Guide to Elliptic Curve Cryptography*

[14] J.Silverman, *An Introduction to the Theory of Elliptic Curves*, Brown University and NTRY Cryptosystems, Inc., Summer School on Computational Number Theory and Application to Cryptography University od Wyoming, USA, 2006.

[15] Marc Joe, *Fault Attacks on Elliptic Curve Cryptosystems*, Thomson Security Labs Atlanta, USA, 2009.

[16] J. H. Silverman, *The Arithmetic of Elliptic Curves* (2nd ed.), Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 2009.