Univerzitet Crne Gore
Prirodno-matematički fakultet

Ilir Čapuni

Kriptografija u modelu izračunljivosti nad poljem racionalnih brojeva

Magistarski rad

Podgorica, 2006.

Univerzitet Crne Gore
Prirodno-matematički fakultet

Ilir Čapuni

Kriptografija u modelu izračunljivosti nad poljem racionalnih brojeva

Magistarski rad

Podgorica, 2006.

PODACI I INFORMACIJE O MAGISTRANTU
Ime i prezime: Ilir Čapuni
Datum i mjesto rođenja: 20.02.1978. godine, Bar
Naziv završenog osnovnog studijskog programa i godina diplomiranja: Prirodno-matematički fakultet, Smjer primjenjene matematike i računarstva, 2003.

INFORMACIJE O MAGISTARSKOM RADU
Naziv postdiplomskog studija: Računarske nauke
Naslov rada: Kriptografija u modelu izračunljivosti nad poljem racionalnih brojeva
Prirodno-matematički fakultet

UDK, OCJENA I ODBRANA MAGISTARSKOG RADA
Datum prijave magistarskog rada: 17.04.2006. godine
Datum sjednice Vijeća Prirodno-matematičkog fakulteta na kojoj je prihvaćena tema: 18.04.2006. godine

Komisija za ocjenu teme i podobnosti magistranta:
prof. Dr Žarko Mijajlović,
prof. Dr Slobodan Vujošević,
doc. Dr Milenko Mosurović

Mentor: prof. Dr Žarko Mijajlović

Komisija za odbranu rada:
prof. Dr Žarko Mijajlović,
prof. Dr Slobodan Vujošević,
doc. Dr Milenko Mosurović

Lektor: prof. Dr Slobodan Vujošević
Datum odbrane
Datum promocije

Predgovor

Moderna kriptografija se bavi bezbjednim prenosom podataka preko nesigurnog komunikacionog kanala. Ona se obično bazira na klasičnom (Turingovom) modelu izračunljivosti, gdje se podaci obično predstavljaju pomoću nizova 0 i 1. Sigurnost nekog kriptografskog protokola ili kriptografskog primitiva bazira se na jazu koji postoji(?) između klasa složenosti izračunavanja. Osnovni kriptografski primitivi su jednosmjerne funkcije, odnosno funkcije koje se "lako" računaju, ali se "teško" invertuju. U klasičnom modelu, nije još pokazano da one postoje.

Pojam izračunavanja je kompatibilan i sa drugim oblicima reprezentacije podataka. Recimo klasične geometrijske konstrukcije pomoću lenjira i šestara jesu jedan vid izračunavanja pomoću kojih su postavljeni temelji matematike u antička vremena, kada se matematika zasnivala prevashodno na geometrijskim razmatranjima i konstrukcijama a brojevi shvaćeni kao duži.

Pored Turingovog modela izračunljivosti (i njemu ekvivalentnih modela), postoje i drugi modeli izračunljivosti, od kojih su posebno interesantni modeli nad poljima realnih i kompleksnih brojeva. Blum, Shub i Smale su 1989. godine predstavili jedan opšti model izračunljivosti nad proizvoljnim prstenom/poljem i specijalno dali neke konkretne odgovore o izračunljivosti realnih brojeva. Sve do pojave ovog modela, u konkretnim realizacijama, realni brojevi su predstavljeni pomoću racionalnih brojeva koji se kodirani pomoću nizova 0 i 1. U BSS (Blum - Shub - Smale) modelu, realan broj se ne kodira već se smatra jednim entitetom nad kojim se vrše neke operacije.

U ovom radu razmatramo problem mogućnosti razvoja kriptografije na BSS modelu izračunljivosti nad poljem $\mathbb{Q}$. Zapravo, razmatramo pitanje da li se u jednom slabom BSS modelu može na bezbjedan način preko nesigurnog kanala prenositi jedan realan broj, a potom i jedan kompleksan broj. U uvedenom modelu, za $r \in \mathbb{Q}$, funkcija $r \mapsto r^2$. Mada je to dobar znak da je BSS model povoljan teren za razvoj teorijske kriptografije, u ovom radu pokazaćemo da identifikacioni protokoli postoje, ali da je enkripcija (a time i čitav niz drugih dvostranih protokola), u slučaju kada sve strane u komunikaciji (pošiljalac, primaoc i napadač) imaju neograničenu ali konačnu moć izračunljivosti, nemoguća(e).

Motiv za ova razmatranja, bio je rad [3] tvoraca RSA sistema enkripcije sa javnim ključem Ronalda Rivesta i Adi Shamira, u kojem se oni pitaju da li, koristeći konstrukcije lenjirom i šestarom, u modelu u kome su podaci predstavljeni pomoću uglova i duži, može uspostaviti sigurna komu-

nikacija. Jednosmjerna funkcija nad uglovima u ovom modelu je recimo funkcija $f(x) = 3 \cdot x$ jer znamo da je trisekcija ugla pomoću lenjira i šestara nemoguća za skoro sve uglove.

U prvom poglavlju, predstavljamo osnovne probleme kriptografije i trenutno stanje njenog razvoja u Turingovom modelu. Potom, dajemo opis BSS modela nad proizvoljnim prstenom i potrebne modifikacije tog modela za korišćenje u kriptografiji. U četvrtom poglavlju bavimo se kriptografijom pomoću lenjira i šestara. Konstrukcije lenjirom i šestarom modelirani su pomoću jedne specijalne mašine koju smo nazvali *pitagorejska BSS mašina.* Na kraju, daju se neka otvorena pitanja.

Osnovna verzija ovog rada predstavljena je u konferenciji Foundations of Computational Mathematics '05 u Santanderu, od 29.06.2005. do 9.06.2005. godine pod naslovom "Cryptography in BSS Computational Model". Tokom i poslije ove konferencije, prof. Klaus Meer i prof. Felipe Cucker su mi pomogli u definisanju odgovarajućeg modela i dali neke korekcije u dokazima glavnih tvrđenja za šta im dugujem posebnu zahvalnost.

Ovom prilikom, želim da izrazim moju zahvalnost mom profesoru Slobodanu Vujoševiću. On se u mom životu u potpunosti uklopio i kao drag prijatelj i kao referentan naučnik na koga se čovjek uvijek može osloniti. Mom mentoru prof. Žarku Mijajloviću posebno zahvaljujem na stalnoj podršci, stalnim savjetima, dobroj literaturi i dobrim preporukama za dalje usavršavanje. Jedino komunicirajući s njim, dobio sam potpunu sliku moje sfere interesovanja – teorije računarstva u velikom i potpunu sliku života kao naučnika. To je osoba koja razumije sve ono što kažem (čak i kada ja samog sebe ne razumijem u potpunosti). Otkrio sam da je nemoguće provesti sa njim 5 minuta a da čovjek od njega ne nauči nešto novo ili ne razjasni neku nedoumicu. U zadnjih par godina, evoluriao sam i kao naučnik i kao čovjek. Poseban doprinos tom evolutivnom procesu imao je prof. Miodrag Perović, čiji sam asistent na predmetu Analiza 2 bio tokom akademskih godina 2004/05 i 2005/06 . On je neiscrpan izvor za nekoga ko pretendira da se bavi matematikom. Aktivno i pasivno, on je mnogo uticao na kvalitet ovog rada u pozitivnom smislu. Posebnu zahvalnost dugujem svim profesorima Prirodno-matematičkog fakulteta u Podgorici, od kojih posebno izdvajam Veselina Perića, Davida Kaljaja, Biljanu i Sinišu Stamatovića i Izedina Krnića. Naravno, rad na ovoj instituciji mi nije teško pao, djeljeći kabinet, iskustva, probleme i rješenja sa Darkom Mitrovićem i družeći se sa tako dobrim kolektivom kao što je kolektiv ovog fakulteta.

Konačno, zahvaljujem se mojoj porodici za neograničenu podršku tokom

čitavom mog školovanja, i Fondaciji Konrad Adenauer koja je podržala moje magistarske studije.

Podgorica, 1.05.2006. godine

Abstract

Most of modern cryptography is based on the classical (Turing) model of computation, where data are represented as sequences of bits. The most basic primitives in cryptography are "one-way functions" - the functions that are "easy" to compute but "hard" (on average) to invert. Though these primitives are widely used, there is no proof of their existence in this classical setting.

Motivated by the work of Rivest, Shamir and Burmester [3], in this work we address the question weather is possible to establish cryptography in other model of computation where data are not bits but elements of an arbitrary ring/field. To be more precise, we address the possibility of the development of cryptography on the BSS (Blum, Shub & Smale) computational model over the field $\mathbb{Q}$.

First, we make some modifications of the classical BSS machines for use in cryptography and then we show that in this model, one- way functions exist. In the search of cryptographic protocols that exist in this model, we show that zero-knowledge identification protocol and zero-knowledge authentication protocols do exist. Existence of one-way functions, identification protocols and authentification protocols present a good indication that maybe public-key encryption scheme could also be established. Unfortunately, we show that this is not true. Modeling the state of knowledge of each party as the field that he/she could generate and giving unbounded computational power to all parties, we show that all parties using the public key encryption have the same state of knowledge.

In the first chapter we present some background of cryptography and address the need and motives for switching to another computational model. In the second chapter we present the classical Blum, Shub & Smale computational model and give some examples of such machines. The third chapter presents the core of this work. In this chapter the authentication protocol is an original result. In the fourth chapter, constructions with ruler and compass are modeled as algebraic operations. We define a weak version of BSS model over the field $\mathbb{C}$ which simulates constructions by ruler and compass without the possibility of finding a square root. We show that in this model the identification protocol could be established, while public key encryption scheme does not exist as was expected. We conjecture the same to be true in the model (with oracles) which completely simulates constructions by ruler

and compass. The summary and some open questions are given in the last chapter.

Sadržaj

Poglavlje 1

Uvod

Kriptografija se bavi komunikacijom u prisustvu napadača (prisluškivača), tj. komunikacijom na nesigurnom kanalu. Ona obuhvata široku lepezu konkretnih problema kao što su enkripcija, autentifikacija, distribucija ključeva, identifikacija itd.

Moderna kriptografija daje teorijsku osnovu koja omogućuje da precizno shvatimo suštinu ovih problema, kako ocjeniti protokole koji su dizajnirani da bi riješili te probleme, i kako kreirati protokole na čiju sigurnost se možemo osloniti.

1.1 Osnovni problemi sa kojima se kriptografija bavi

U literaturi se obično legalni korisnici u nekom protokolu zovu Alisa i Bob, dok napadače predstavlja Eva[1]. Originalna poruka se obično naziva *otvoren tekst* i označava se sa m, dok se sa c označava šifrovana poruka ili kraće *šifrat*.

1.1.1 Problem enkripcije – sistem sa tajnim ključem

Ana želi da Bobu proslijedi tajnu poruku preko linije koja može biti prisluškivana.

Osnovno rješenje ovog problema je *enkripcija sa privatnim ključem*. U ovom načinu enkripcije, Alisa i Bob se moraju susresti prije početka prenosa

[1]Skraćeno od *eavesdropper*- osoba koja prisluškuje, remeti privatnost itd.

poruka, pri čemu se moraju dogovoriti o algoritmu enkripcije $\mathcal{E}$, o algoritmu dekripcije $\mathcal{D}$ i o informaciji S koja mora biti tajna. S ćemo nadalje zvati *zajednički tajni ključ*. Osoba koja prisluškuje može znati oba algoritma $\mathcal{E}$ i $\mathcal{D}$, ali nikako tajni ključ S.

Alisa šifrira svoju poruku m upotrebljavajući $\mathcal{E}$ i S. Dakle, Alisa kroz nesiguran kanal šalje $c = \mathcal{E}(S, m)$. Po prijemu, Bob, uzima tajni ključ S i upotrebom algoritma $\mathcal{D}$ dobija nazad originalnu Alisa poruku, tj. $m = \mathcal{D}(S, c)$. Osoba koja prisluškuje, neznajući S, ne može izračunati originalnu poruku m od poruke c koja ja putovala kanalom.

1.1.2 Problem enkripcije - sistem sa javnim ključem

Pretpostavka da su se Alisa i Bob već prethodno sreli da bi se dogovorili za ključ jeste ograničavajući faktor u komunikaciji (sam susret Alise i Boba) i u sigurnosti (limitirana mogućnost promjene ključa u slučaju da dođe do krađe ključa).

Uvođenjem kriptografije sa javnim ključem tokom '70-ih godina prošlog vijeka, odbačena je pretpostavka da Alisa i Bob moraju dijeliti isti ključ da bi mogli šifrirati poruke. Primaoc poruke (Bob), objavljuje autentičnu[2] informaciju (koja se zove *javni ključ*) za bilo koga uključujući i napadače, pošiljaoca (Ani), i sve ostale zainterosvane pošiljaoce.

U ovom sistemu, bilo ko može pročitati Bobov javni ključ, može njemu poslati šifrovanu poruku, a da se sa njim nijesu prethodno morali susresti (da bi se dogovorili o ključu). Ovakvi sistemi sada rade ne samo za jedan par korisnika (Alisu i Boba), već za sve ostale osobe koji znaju Bobov javni ključ i koji bi tajno komunicirali s njim. Dakle, primalac poruke- Bob, u nekom javnom direktorijumu (recimo telefonskom imeniku, oglasima, web-u itd.) objavljuje svoj javni ključ, i njegovi korespondenti, poruke namjenjene njemu šifriraju pomoću ovog ključa. On zatim, ima drugi – *tajni ključ* i sve poruke otvara pomoću njega.

1.1.3 Definicije sigurnosti i model napadača

Šta se stvarno podrazumijeva pod pojmom "sigurnost"? Sigurnosni zahtjevi se razlikuju od protokola do protokola. Najosnovniji preduslov sigurnosti za

[2]Kada se kaže da je informacija autentična, misli se da je pošiljaocu data garancija da je ta informacija objavljena od legalnog primaoca.

enkripciju je da napadač koji vidi šifrat i zna postupke enkripcije i dekripcije ne može restaurirati otvoreni tekst. Međutim, lista uslova se proširuje i sa nekim "poželjnim" osobinama od kojih izdvajamo:

1. Parcijalne informacije o poruci se teško računaju iz šifrata.
2. Detekcija prostih, ali korisnih podataka o prenosu poruka (kao što je podatak da li je jedna poruka poslata dvaput) mora biti teško izvodljiva.
3. Prednje osobine moraju da se realizuju sa velikom vjerovatnoćom.

Do sada smo pretpostavili da napadač: može da ukrade šifrat tokom prenosa podataka na nekom nesigurnom kanalu, može čitati javno dostupne podatke, može generisati šifrate bilo koje poruke i da ima određenu računsku moć. Napadač ovakvog tipa zove se *pasivan napadač.*

U realnosti, napadač može da zaustavi prenos podataka ili mijenja podatke tokom prenosa, ukrade identitet tokom identifikacije itd. Ovakav napadač zove se *aktivan napadač.*

1.1.4 Problem identifikacije

Alisa želi da dokazati svoj identitet Bobu kako bi pristupila nekom resursu.

Sheme identifikacije se najčešće upotrebljavaju u velikim distribuiranim sistemima, u kojima se korisnici ne poznaju međusobno. U takvim sistemima, neko želi da jednom korisniku dozvoli da drugima potvrdi svoj identitet. Pokazuje se da su sheme identifikacije tijesno povezane sa dokazima znanja (vidi [5]).

Problem identifikacije je najbolje približiti pomoću jednog opisnog primjera. Shema identifikacije se sastoji od *javne datoteke* koja sadrži podatke o svim korisnicima i *identifikacionog protokola.* Svaki javni podatak sadrži ime (ili identitet) korisnika i neke pomoćne podatke za identifikaciju. Javni fajl se kreira i održava od strane povjerljive strane koja garantuje autenticitet podataka (tj. da su svi podaci o određenom korisniku ubačeni samo od strane korisnika čije ime stoji na tom polju). Svi korisnici mogu čitati javni fajl tokom čitavog vremena.

Pretpostavimo sada da Alisa želi da Bobu dokaže da je to ona koja priča sa njim. Bob će Alisi postaviti nekoliko pitanja na koja Alisa mora da odgovori ("čik pogodi" sistem).

Rješenje problema mora da je takvo da je Alisa uvjek u stanju da ubijedi Boba da je to stvarno ona, a da pritom, niko drugi ne može prevariti Boba i predstaviti se kao Alisa.

Normalno, Alisa mora da svoj javni identitet, dobijen na slučajan način, drži kao tajnu. Tokom identifikacije, Ana će svakako koristiti ovaj podatak, ali to mora biti urađeno tako da niko drugi ne može da joj ukrade identitet poslije, tj. da se neko predstavi kako ona.

Dakle, identifikacioni protokoli, imaju svojstvo da čak i ako napadač (Eva) sazna dio dokaza identiteta, taj dio nije dovoljan da Boba ubijei da je to Alisa. Ovo svojstvo se ne može postići sa tradicionalnim mehanizmom lozinki.

1.1.5 Zero-knowledge protokoli

Interaktivni protokol čine dvije strane: dokazivač i verifikator. Verifikator i dokazivač komuniciraju i na kraju, verifikator treba da jedan od dva moguća odgovora: prihvata ili odbije dokaz.

Ključna ideja je da se opšti problem dvostranih protokola svodi na prostiji problem: Kako može Alisa da dokaže Bobu da je $x \in L$ tako da ne otkrije drugo znanje sem same činjenice da je $x \in L$.

U zero-knowledge protokolima postoji mogućnost prevare: prevarant (Eva) je obično u stanju da da daje korektne odgovore na neka pitanja verifikatora. Protokoli moraju da budu takvi da odgovor na neko pitanje ne otkriva informacije .

1.1.6 Zero-knowledge autentifikacija

Sheme autentifikacije poruka omogućavaju stranama koje znaju neki zajednički tajni ključ da budu sigurni u integritet podataka. Cilj je da primalac poruke bude siguran da su prenešeni podaci poslati od legitimnog pošiljaoca. Često se pogrešno problem autentifikacije mješa sa problemom enkripcije. Bitno je naglasiti da nas ne zanima tajnost podataka - podatak može čak biti u otvorenom obliku. Nas zanima napadač koji može da mijenja sadržaj poruke.

1.2 Temelji kriptografije

Po definisanju izračunljivosti početkom '30.-ih godina dvadesetog vijeka, matematičari su se pretežno bavili pitanjima da li je neka funkcija izračunljiva ili ne, tj. da li je neki problem odlučiv ili ne. Do '60.-ih godina tog vijeka, matematičari su se pretežno bavili klasifikacijom problema na odlučive i neodlučive. Tek pošto su prvi elektronski računari počeli da se naveliko koriste, počelo je i razmišljanje u terminima računarskih resursa i računarskog vremena, tj. u terminima teorije složenosti. Temelje teorije složenosti uveo je Manuel Blum, uvodeći funkciju mjere složenosti, i potom Stephen Cook i Leonid Levin sa svojom teoremom o kompletnosti problema zadovoljivosti, tj. pojavom dvije glavne klase složenosti: klase $\mathcal{P}$ i klase $\mathcal{NP}$.

Moderna kriptografija se zasniva na jazu između efikasnih algoritama za enkripciju za legitimne korisnike (Alise i Boba) i neizvodljivosti dekripcije za napadača (Evu). Dakle, u terminima sistema enkripcije, šifrovanje mora da bude "lako" ali razbijanje bez znanja ključa mora biti težak problem. Ovim zapravo tražimo neke određene primitive koje u sebi imaju neka svojstva teškoće računanja. Najosnovniji od ovih primitiva jesu jednosmjerne funkcije, generatori pseudo-slučajnih brojeva i familije pseudo-slučajnih funkcija.

Obično se nekorektno misli da se kriptografija bavi kreiranjem šifara koje je nemogućnost "razbiti", tj. definisanjem neke funkcije koja se lako računa ali se nikako ne može invertovati. U terminima izračunljivosti, to su funkcije koje se lako računaju, ali čije je invertovanje nemoguće tj. neizračunljivo (kao recimo halting problem). Međutim, u kriptografiji se obično moć računanja strana u komunikaciji ograničava na neki razuman način.

1.3 Problemi kriptografije u Turingovom modelu

Gotovo čitava kriptografija se bazira na klasičnom modelu izračunljivosti gdje se obično podaci predstavljaju kao nizovi 0 i 1. Poznato je da u ovom modelu, još nije određena separacija između klasa $\mathcal{P}$ i $\mathcal{NP}$.

Čitava kriptografija u ovom modelu, bazira se na nekim empirijskim i nedokazanim pretpostavkama. Recimo, sigurnost RSA kriptosistema, bazira se na takozvanoj RSA hipotezi, ili recimo na hipotezi da je faktorizacija velikih brojeva i dalje vrlo težak problem.

Jedna od najbitnijih otvorenih pitanja kriptografije u ovom modelu je

da li jednosmjerne funkcije uopšte postoje. Pokušaji da se dokaže postojanje ovih funkcija su se pokazali neuspješnim čak i pod pretpostavkom $\mathcal{P} \neq \mathcal{NP}$. I pored prednjeg, u upotrebi je jedan ogroman skup kandidata za jednosmjerne funkcije, ali dokaze da su one stvarno jednosmjerne još nema na vidiku.

Dalje, u ovom modelu nemoguće je da Bob Alisi na siguran način pošalje jedan realan a time i kompleksan broj, jer su, znajući da racionalni brojevi dobro aproksimiraju realne brojeve, realni brojevi u ovom modelu predstavljeni racionalnim brojevima, a racionalni brojevi se dalje kodiraju pomoću nizova 0 i 1.

1.4 BSS model izračunljivosti: model nad proizvoljnim prstenom

U cilju rješenja problema $\mathcal{P}$ vs.$\mathcal{NP}$ i u cilju pravilnog utemeljenja numeričkih metoda, Lenore Blum, Mike Shub i Steven Smale, 1989. godine, predstavili su model gdje podaci više nijesu bitovi, već su elementi nekog proizvoljnog prstena (ili polja) R. Recimo, R može biti polje realnih brojeva, polje kompleksnih brojeva, ili pak prsten $\mathbb{Z}_2$. Postignuto je to da ako se stavlja $R = \mathbb{Z}_2$ dobije Turingov model i ne samo to, već je dobijena i jedna bogata teorija izračunljivosti nad realnim i kompleksnim brojevima.

Vidjećemo da u ovom modelu, jednosmjerne funkcije postoje tj. da nema potrebe da sigurnost kriptografskih paradigmi baziramo na nedokazanim hipotezama.

U ovom modelu, slutimo da se mogu razviti kriptografski metodi gdje se jedan realan broj može prenijeti na siguran način preko nesigurnog komunikacionog kanala.

1.5 Organizacija rada i naši rezultati

Cilj ovog rada nije da se bavi sa praktičnim detaljima (recimo kako da praktično predstaviti podatke pomoću realnih brojeva, uglova i duži), već da razmotrimo mogućnost razvoja kriptografije u širem modelu.

Smatraćemo recimo, da su nam podaci neki realni brojevi ili kompleksni brojevi, i da Alisa i Bob komuniciraju tako što jedan drugom šalju te objekte.

U drugom poglavlju, predstavljamo BSS model izračunljivosti sa potrebnom teorijom i nekim primjerima mašina.

U trećem poglavlju – koje je centralno u ovom radu, predstavljamo kriptografiju u BSS modelu. Prvo se mašine malo modifikuju, a potom se redom pokazuje da je u ovom modelu moguće definisati zero-knowledge identifikacioni protokol i protokol autentifikacije, a zatim se pokazuje da je definisanje sistema šifriranja sa javnim ključem nemoguće. Protokol autentifikacije predstavljen u ovom poglavlju je originalan rezultat.

U četvrtom poglavlju, primjenjujemo rezultate iz prethodnog poglavlja i bavimo se kriptografijom u pitagorejskoj ravni koja je i bila motiv ovog rada.

U zaključnom – petom poglavlju, rezimiramo rezultate i predstavljamo neka preostala otvorena pitanja.

Poglavlje 2

Model izračunljivosti nad proizvoljnim prstenom

U ovom poglavlju predstavljamo opšti model izračunljivosti koji je predstavljen 1989. godine od strane L.Blum, M. Shub i S. Smale-a. Detaljan prikaz teorije izračunljivosti nad ovim modelom, dat je u monografiji [2]. U daljem tekstu, ovaj model ćemo kratko nazvati BSS model.

2.1 Mašine nad prstenom ili poljem R

Pretpostavljamo da je R komutativan prsten ili polje, (po mogućnosti uređeno) sa jedinicom. *Mašina* M nad R ima sljedeća svojstva:

- Mašini M se pridružuju ulazni i izlazni prostori, koji su zapravo R^∞ (disjunktna unija R^n, $n \geq 0$);
- Na visokom nivou, mašina M je slična sa Turingovom mašinom: ima *dvostranu beskonačnu traku* koja je podjeljena na *ćelije*, ima *glavu za čitanje i pisanje* koja može da *vidi* fiksiran broj k_M uzastopnih ćelija istovremeno. U svakoj ćeliji se može smjestiti jedan element prstena R.
- Unutrašnjost mašine čini *program* - konačan usmjeren graf sa 5 tipova čvorova: ulazni, izlazni, računajući, pomjerajući i čvorovi grananja. Svakom čvoru se pridružuje *operacija čvora* i *pokazivač na sljedeći čvor*:

1. Operacija g_i pridružuje se *ulaznom čvoru* i. To je zapravo jedno linearno preslikavanje koje uzima elemente $\vec{x} = (x_1, \ldots, x_k)$ iz ulaznog prostora R^∞ i stavlja, svako $x_i, (i = 1, \ldots, k)$ u uzastopnim ćelijama na traci, počev od krajnje lijeve ćelije na pogledu mašine M. Za ulazni čvor, postoji jedinstven izlazni čvor $i_1 \neq i$.

2. Svaki *računajući čvor* ima ugrađenu polinomijalnu ili racionalnu funkciju $g_\eta : R^n \to R^m$, $n, m \leq k_M$.[1] Za date elemente $x_1, x_2, \ldots, x_n$ u prvih n ćelija pogleda mašine M, pridružena operacija se označava g_η, i ona u j-toj ćeliji na pogledu mašine M stavlja $g_\eta^j(x_1, \ldots, x_n)$, $(j = 1, \ldots, m)$. Za svaki računajući čvor, postoji jedinstveni sljedeći čvor η_1.

3. Svakom *čvoru grananja* η pridružuje se operacija identiteta. Postoje dva moguća izlazna čvora: η'_L i η'_R, zavisno od elementa u krajnjoj lijevoj ćeliji l u pogledu mašine M. Ako je $x_l = 0 (\geq 0$ ako je R uredjen), onda je $\eta' = \eta'_R$. Ako je $x_l \neq 0 (\leq 0)$, onda je $\eta' = \eta'_L$.

4. Svakom pomjerajućem čvoru σ, pridružuje se identitet, i postoji jedinstven sljedeći čvor σ'. Razlikuju se desnopomjerajući čvorovi σ_R koji pogled mašine M pomjeraju za jednu ćeliju desno, i lijevopomjerajući čvorovi σ_L koji taj pogled pomjeraju za jednu ćeliju ulijevo.

5. Izlaznom čvoru N, pridružuje se linearno preslikavanje g_η koja projektuje sadržaj trake na izlazni prostor R^∞. Izlazni čvor N nema sljedeći čvor.

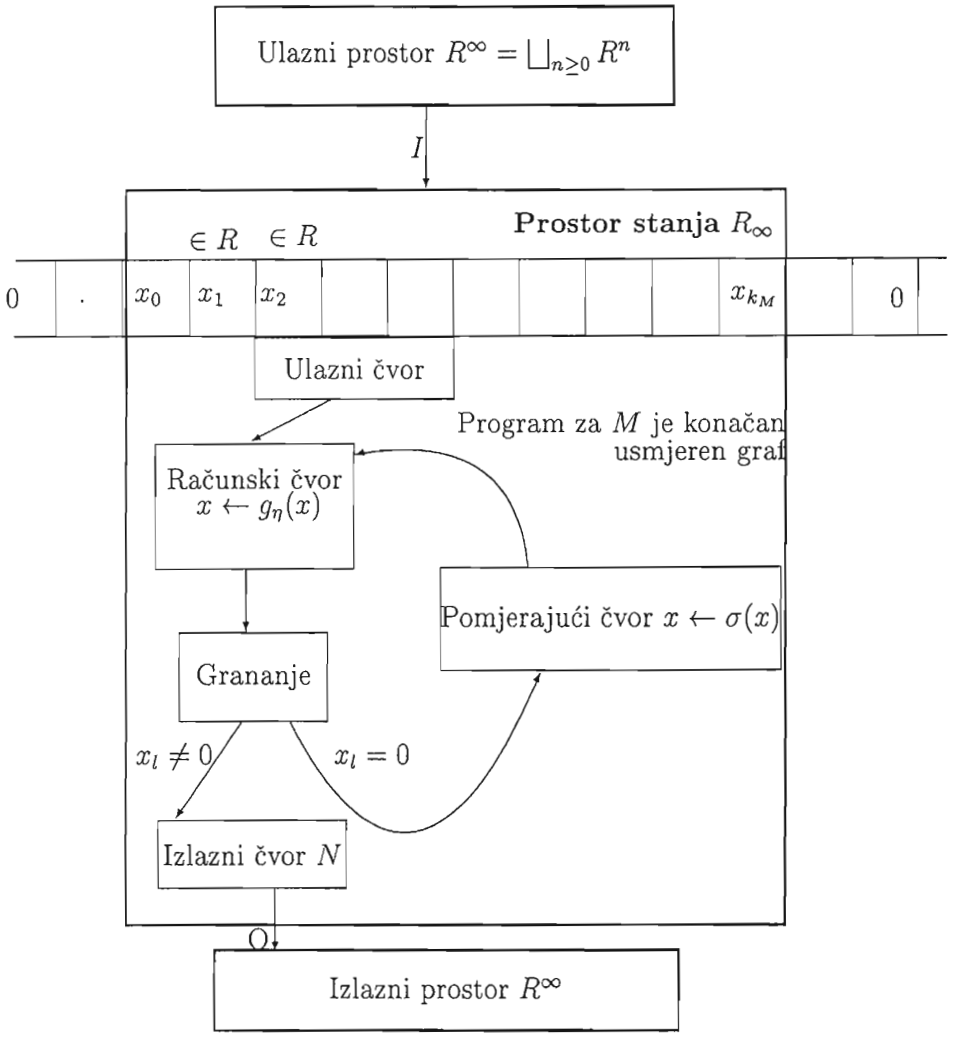
Definicija 2.1.1 *Izračunljive funkcije nad R su ulazno-izlazne funkcije ϕ_M mašine M nad R. Za $x \in R^\infty$, $\phi_M(x)$ je definisana ako se izlazni čvor N može dostići obilazeći čvorove programa kada je ulazni podatak x. U tom slučaju, $\phi_M(x)$ je izlazni podatak $y \in R^\infty$.*

Napomena 2.1.2 *Mada je mašinin pogled na traku u bilo kom trenutku konačan (veličine k_M), pomjerajući čvorovi omogućavaju mašini da čita i djeluje nad svim ulazima iz R^n, za svako n. Ovim, možemo modelirati algoritme koji su definisani ravnomjerno za ulaze bilo koje dimenzije. Primjećujući ovo, možemo konstruisati univerzalne (progamabilne) mašine nad R.*

[1] Mašina nad R može imati *konačan broj ugrađenih konstanti* koji su elementi od R.

Napomena 2.1.3 *Ako je $R = \mathbb{Z}_2$, onda naš model izračunljivosti postaje klasičan Turingov model.*

Definicija 2.1.4 *Stepen mašine M je maksimum stepena svih polinoma koji se koriste u programu.*



Slika 1. Mašina nad prstenom ili poljem R - pogled iznutra.

2.2 Primjeri BSS mašina

Neka je R proizvoljan komutativan prsten sa jedinicom (recimo prsten $\mathbb{Z}$ ili polja $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$). Razmatramo sljedeći problem:

> Za date $c, x_1, x_2, \ldots, x_n \in R$, odlučiti da li postoji neprazan podskup $S \subset \{1, 2, \ldots n\}$ tako da $\sum_{i \in S} x_i = c$.

Obično se ovaj problem naziva *problem ranca* pri čemu je c zapravo njegov kapacitet a x_i su težine datih stvari koje se moraju smjestiti u rancu. Pitamo se da li postoji spisak stvari kojima možemo napuniti ranac.

Daćemo dvije mašine koje su dobre ilustracije moći i oblika izračunavanja u ovom modelu.

Primjetimo da ovaj problem možemo modelirati ovako: definišemo

$$K_n = \{x \in R^n | \exists b \in \{0,1\}^n \text{ tako da } \sum_{i=1}^{n} b_i x_i = c\},$$

i za dato $x \in R^n$ pitamo da li je $x \in K_n$.

Konstruišimo sada prvu mašinu koja odgovara na postavljeno pitanje.

Opis postupka: Za dato $x \in R^n$, generisati sve nenulte elemente $\{0,1\}^n$ i izračunati $\sum_{i=1}^{n} b_i x_i$. Ako je ova suma c, onda stani i na izlazu daj 1 (da). Inače, stani i na izlazu daj 0 (ne) (slika 2).

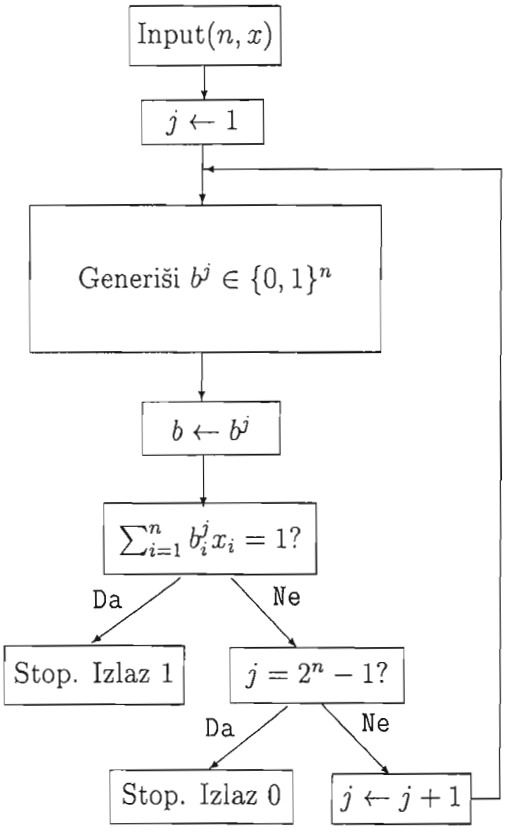
U najgorem slučaju, ovoj mašini trebaće $2^n - 1$ koraka da bi dala tačan odgovor .

Da li možemo konstruisati bolju mašinu od ove? Da li postoji mašina kojoj će trebati polinomijalno mnogo koraka da za dato $x \in R^n$ odluči da li je $x \in K_n$?

Sada dajemo jednu drugu mašinu koja ilustruje duh BSS modela – da se u računskim čvorovima računa vrijednost nekog polinoma.

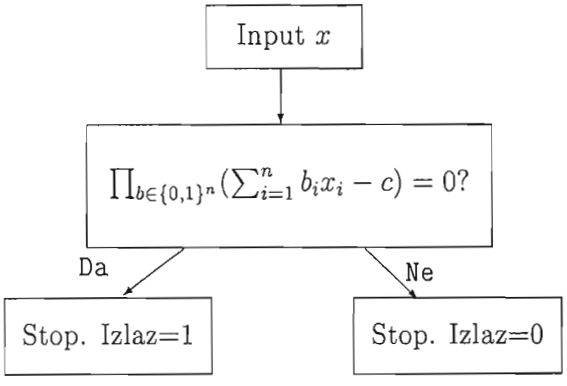
Definišimo polinom $k_n(x) \in R[x_1, \ldots, x_n]$

$$k_n(x) = \prod_{b \in \{0,1\}^n} (\sum_{i=1}^{n} b_i x_i - c)$$



Slika 2. Mašina koja problem ranca rješava prebrojavanjem. Ona ima čvor u kojem se za dato (n, j) generiše j-ti nenulti niz iz $\{0,1\}^n$. Zatim, za tu sekvencu, mašina provjerava da li je $\sum_{i=1}^n b_i^j x_i = 1$.

i neka je $V_{k_n} = \{x \in R^n | k_n(x) = 0\}$. Onda je $V_{k_n} = K_n$. Dakle, konstruisaćemo algebarsku mašinu, koja će u jednom koraku dati odgovor na postavljeno pitanje. Ona ima ugrađen računski čvor koji računa $k_n(x)$ u jednom koraku (slika 3.).



Slika 3. Algebarska mašina za rješenje problema ranca.

Stepen ove mašine je dakako $2^n - 1$. Time smo napravili kompromis između eksponencijalnog pretraživanja i evaluacije polinoma eksponencijalnog stepena po n.

2.3 Završne napomene

Podsjetimo, RAM model je dao istu klasu izračunljivih funkcija kao i Turingov model, pa se u teoriji algoritama obično posmatraju RAM mašine umjesto Turingovih. Na istovjetan način, BSS mašine nad prstenom R možemo shvatiti kao RAM mašine u čijim se registrima mogu smjestiti proizvoljni elementi prstena R i nad njima je moguće obavljati operacije prstena u konstantnom vremenu.

Pažljivom analizom ovog modela, primjećujemo da je ovaj model univerzalan ali i previše idealan.

Prirodno je postaviti pitanje da li je ovim modelom dobijena šira klasa izračunljivih funkcija, odnosno da li vrijedi Church-ova teza. Naravno, odgovor je da smo ovim modelom proširili skup izračunljivih funkcija recimo sa jednom klasom realnih funkcija (ako je $R = \mathbb{R}$) koje su u Turingovom modelu bile neizračunljive. Ali, ako je $R = \mathbb{Z}_2$, onda dobijamo istu klasu izračunljivih funkcija kao i u Turingovom modelu.

Halting skup Ω_M mašine M je skup svih ulaznih podataka na kojima se M zaustavlja. Pokazuje se da su halting skupovi u BSS modelu prebrojive unije semi-algebarskih skupova[2], dok su izračunljive funkcije dio po dio polinomijalne (ili dio po dio racionalne ako je R polje).

Razmotrimo slučaj kada je $R = \mathbb{R}$. U praksi, zahtjev da se u svakoj ćeliji (registru) može smjestiti proizvoljan realan broj sa beskonačnom tačnošću može izgledati previše idealno. Isto tako, idealno izgleda i zahtjev da se računske operacije obavljaju u jednom koraku u konstantnom vremenu. Postoje razne modifikacije ovog modela koje su objasnjenje u [2]. Te se modifikacije obično dobijaju slabljenjem ili pak odbacivanjem nekih uslova. Dobijene mašine se obično zovu *slabe* mašine a odgovarajući modeli slabim. Recimo u slabom BSS modelu uvedenom u [6], odbacuje se pretpostavka da mašine vrše operacije nad R u konstantnom vremenu. Interesantno je da se u ovom dobijenom slabom modelu, dobija separacija klasa $\mathcal{P}_W$ i $\mathcal{NP}_W$.

[2]Za skup $S \subset R^n$ kažemo da je *osnovni semi-algebarski skup* nad R u slučaju da je R uređen (ili *osnovni kvazi-algebarski skup* ako je R neuređen prsten), ako je S skup elemenata od R^n koji zadovoljavaju konačan sistem polinomijalnih jednakosti i nejednakosti nad R. *Semi-algebarski (ili kvazi - algebarski) skup* je konačna unija osnovnih semi-algebarskih (ili osnovnih kvazi- algebarskih) skupova

Poglavlje 3

Kriptografija u BSS modelu

U ovom poglavlju, pokazaćemo da klasičan BSS model nije pogodan za kriptografiju i uvešćemo neka ograničenja i dobiti jedan slabi BSS model. Vidjećemo da su u ovom modelu rješena samo dva problema kriptografije - identifikacija i zero-knowledge protokoli, dok je enkripcija sa javnim ključem nemoguća.

3.1 Adaptacija osnovnog BSS modela

Sve strane počinju izračunavanja od nule i jedinice, pomoću standardnih operacija iz skupa $\{+, -, *, /\}$. Dozvoljeno je izvršavanje neograničeno ali konačno mnogo operacija. Dakle, na ovaj način, mašina može generisati bilo koji racionalan broj. Smatramo da je *stanje znanja* zapravo polje koje se može generisati pomoću mašine. U našem slučaju, stanje znanja za sve strane u komunikaciji je polje racionalnih brojeva, što zapravo znači da u ovom modelu ne postoje tajne, jer se sve može izračunati. Ilustrujmo prednje jednim primjerom.

Primjer 3.1.1 *Pretpostavimo da se komunikacija obavlja nad nekim prebrojivim poljem F pri čemu Alisa i Bob žele da sakriju element s tog polja, i pretpostavimo da Eva posjeduje generatore tog polja. Pretpostavimo dalje da postoji neki javno dostupan algoritam verifikacije za s, tj. da postoji neka javno dostupna izračunljiva funkcija $p : F \longrightarrow \{0, 1\}$ tako da je $p(x) = 1$ ako i samo ako $x = s$. Onda, obzirom da posjeduje generatore, Eva generiše elemente $f \in F$ sve dok nije ispunjen uslov $p(f) = 1$, tj. kada ona saznaje tajni podatak s. Ovaj napad ćemo nazvati napad prebrojavanjem.*

Napad koji smo predstavili u primjeru, se može izbjeći ako svim učesnicima u komunikaciji dozvoljavamo da izaberu na slučajan način neki konačan realan broj sa ravnomjernom raspodjelom. Međutim, obzirom da je nemoguće izabrati realan broj sa ravnomjernom raspodjelom nad čitavim skupom realnih brojeva, pretpostavićemo da učesnici mogu da izaberu na slučajan način neki broj iz intervala $[a, b]$ gdje su a i b neki predefinisani parametri.

Ovim smo izbjegli napad prebrojavanjem. Stvarno, ako je $\vec{r} = (r_1, \ldots, r_n)$ vektor realnih brojeva, pri čemu su za sve i r_i izabrani slučajno iz intervala $[a, b]$, onda učesnici u komunikaciji mogu izračunati polje $\mathbb{Q}(\vec{r})$. Iako je polje $\mathbb{Q}(\vec{r})$ prebrojivo, Alisa i Bob mogu čuvati tajnu jer je vjerovatnoća da će Eva pogoditi pravi generator tog polja jednaka nuli. Stvarno, ako je $\vec{t} = (t_1, \ldots, t_n)$ onda je $P[\mathbb{Q}(\vec{t}) \cap \mathbb{Q}(\vec{r}) = \mathbb{Q}] = 1$.

Sada se postavlja pitanje da li ćemo pojačati "sigurnost" tj. smanjiti šanse napada ako pretpostavimo da će Alisa i Bob držati u tajnosti interval $[a, b]$? Dalje, da li se smanjuju Evine šanse da pogodi pravi vektor ako se dužina vektora n drži u tajnosti? Konačno, da li su njene šanse smanjene ako n raste i obratno.

Prvo, da napomenemo, da ako pretpostavimo da će Alisa i Bob držati u tajnosti bilo koji podatak mimo standardnih ključeva, onda će se postaviti pitanje sigurnosti dogovora između Alise i Boba na nesigurnom kanalu, tj. problem sigurnog prenosa podataka tokom dogovaranja o ovim parametrima. Štaviše, time ćemo narušiti dogovor u kriptografskoj zajednici da takozvane sigurnosne parametre smatramo lako dostupnim podacima.

Drugo, primjetimo da smo već postigli da je vjerovatnoća Evinog uspjeha, tj. njena prednost nula, pa su dalja razmatranja izlišna.

Odgovorimo ipak na postavljena pitanja. Prvo, ako su brojevi a i b tajni, onda će Eva morati da pogodi iste podatke slučajnim izborom iz realne prave sa ravnomjernom vjerovatnoćom, a već smo konstatovali da je to nemoguće. Ostaje jedino, da se napravi dogovor da a i b budu ograničeni. Ovime, smo samo komplikovali model i problem, a pozitivni efekti su zanemarljivi. Drugo, trivijalno se vidi da je vjerovatnoća da će Eva pogoditi n jednaka nuli.

Na osnovu naprijed iznijetog, možemo pretpostaviti da se izbor slučajnih realnih brojeva radi iz $[0, 1]$.

3.2 Jednosmjerne funkcije u slabom BSS modelu

U skupu najosnovnijih kriptografskih primitiva spadaju *jednosmjerne funkcije*, tj. funkcije koje se lako računaju ali teško invertuju. Prije same definicije jednosmjernih funkcija naglašavamo da se za funkciju ν kaže da je *zanemarljiva* ako za svaku konstantu $c \geq 0$ postoji cio broj k_c tako da $\nu(k) \leq k^{-c}$ za svako $k \geq k_c$. Za mašinu kažemo da je polinomijalna ako za svako $x \in R^n \subset R^\infty$ broj obiđenih čvorova tokom računanja je najviše cn^q za neke fiksirane $c, q \geq 1$. Ovdje je n veličina x.

Definicija 3.2.1 *Funkcija $f : R^\infty \to R^\infty$ je jednosmjerna ako*

1. *Postoji vjerovatnosna polinomijalna BSS mašina*[1] *koja za $x \in R^\infty$ na izlazu daje $f(x)$.*
2. *Za bilo koju vjerovatnosnu polinomijalnu BSS mašinu A, vjerovatnoća da će se generisati tačan x je zanemarljiva.*

Neka je $x \in \mathbb{Q}$. U našem modelu nad $\mathbb{Q}$, funkcija $x \mapsto x^2$ se lako računa pomoću osnovnih operacija polja. Međutim, nemoguće je koristeći iste operacije iz x^2 dobiti x. U ovoj mašini, mogu se generisati slučajni realni brojevi, ali se x nalazi u nekom prebrojivom podskupu skupa $\mathbb{R}$. Dakle,

$$P_{\vec{t} \in [a,b]}[\mathbb{Q}(\vec{t}, x^2) \cap \mathbb{Q}(x) = \mathbb{Q}] = 1$$

tj., vjerovatnoća dobijanja x iz $\mathbb{Q}(x^2)$ je nula, pa je $f(x) = x^2$ jednosmjerna funkcija u ovom modelu.

Napomena 3.2.2 *Kod jednosmjernih funkcija smatra se da napadač nije onemogućen da invertuje funkcije, već da je mala vjerovatnoća da to uradi. Od napadača se ne traži da odredi x, već da odredi neke inverze $y = f(x)$. Naravno, ako je funkcija injektivna, onda jedini takav element je x.*

[1] Polinomijalne mašine imaju jedan tip čvorova više od osnovnog modela u osnovnoj definiciji. Ovi čvorovi, koje nazivamo vjerovatnosnim čvorovima, imaju dva sljedeća čvora i nemaju pridruženo preslikavanje. Kada izračunavanje stiže do ovakvog čvora, ono slučajno sa vjerovatnoćom 1/2 bira sljedeći čvor od dva moguća.

3.3 Primjer identifikacionog protokola

U sekciji 1.1.4., predstavili smo problem identifikacije. Da bi naše izlaganje bilo strogo, moraćemo da preciziramo način kako dvije BSS mašine komuniciraju, odnosno definisati jednu vrstu mašine koja je sposobna da komunicira. Ovakvu mašinu, nazvaćemo *interaktivna BSS mašina* (IBSS mašina).

Definicija 3.3.1 Interaktivna BSS mašina *je BSS mašina koja pored standardnih svojstva ima jednu ulaznu traku samo za čitanje, jednu traku samo za čitanje za slučajne brojeve, jednu komunikacionu traku samo za čitanje, jednu komunikacionu traku samo za pisanje, i jednu izlaznu traku samo za pisanje. Traka za slučajne brojeve sadrži beskonačne nizove elemenata iz R koji su izabrani na slučajan način. Ova traka se može čitati samo s lijeva na desno. Kada kažemo da* mašina bira slučajan broj *mislimo na to da mašina čita sljedeću ćeliju sa ove trake. Sadržaj komunikacione trake samo za pisanje su* poruke poslate *od te mašine, dok sadržaj komunikacione trake samo za čitanje su* primljene poruke.

Definicija 3.3.2 Interaktivni protokol *je uređen par IBSS mašina (A, B) koji dijele istu ulaznu traku: komunikaciona traka samo za pisanje mašine B je komunikaciona traka samo za čitanje mašine A i obratno. Mašine se aktiviraju naizmjenično, dok se mašina B aktivira prva u početku. Tokom aktivnog perioda, mašina vrši neka interna izračunavanja shodno sadržaju traka, i potom piše na njenu komunikacionu traku samo za pisanje. i-ta* poruka *od $A(B)$ je niz koji $A(B)$ piše na komunikacionoj traci tokom i-tog perioda aktivnosti. Potom, mašina se deaktivira i aktivira se druga mašina (naravno ukoliko protokol nije završen). Svaka mašina može prekinuti protokol tako što ne salje nijednu poruku tokom svog perioda aktivnosti. Mašina B* prihvata *(ili odbija) ulazni podatak ulaskom u prihvatajuće (odbijajuće) stanje i prekidom protokola. Prvi član para - A, je neograničena BSS mašina.* [2] Vrijeme računanja *mašine B definiše se kao zbir vremena računanja mašine B tokom aktivnih perioda i ograničena je polinomom po veličini ulazne torke.*

Definicija 3.3.3 *Neka je $L \in R^{\infty}$. Kažemo da L ima* interaktivan sistem dokazivanja *ako postoji IBSS mašina V tako da*

1. *postoji IBSS mašina P tako da (P, V) je interaktivan protokol i za svako $x \in L$ za koje je $size(x)$ dovoljno veliko vjerovatnoća da V prihvata je 2/3 (nad izborom slučajnih brojeva mašine V i P);*

[2] Tj. ona može da napravi neograničeno ali konačno mnogo računskih koraka.

2. *za svaku IBSS mašinu P za koje je (P, V) interaktivan protokol, za svako $x \notin L$ za koje je size(x) dovoljno veliko, vjerovatnoća da V prihvata je veća od 1/3 (kada se vjerovatnoće razmatraju nad izborom slučajnih elemenata mašine V i P).*

IBSS mašine iz prethodne definicije su označene sa V (verifikator) i P (prover- dokazivač). Prvo svojstvo iz zadnje definicije zove se svojstvo kompletnosti, dok se drugo svojstvo naziva svojstvo razumnosti. Identifikacioni protokol mora da ima još i treće svojstvo - svojstvo zero-knowledge tj. da ne otkriva "previše" znanja. Sigurnost ovakvih protokola se oslanja na nemoguqqnost dokazivača da predviđa pitanja verifikatora. Ako se osnovni protokol ponavlja više puta, onda se vjerovatnoća globalne prevare smanjuje.

Dakle, zero-knowledge protokol identifikacije mora imati tri svojstva:

Kompletnost. Dokaz identiteta legitimnog dokazivača (Alise) se uvijek prihvata.

Razumnost. Dokaz identiteta nekog prevaranta se odbija sa nekom fiksiranom vjerovatnoćom.

Zero-knowledge. Ovo svojstvo je jače od tvrđenja da verifikator ne može saznati ništa o tajni. Traži se da nikakva strategija verifikatora ne može izvući bilo koje informacije od dokazivača.

Pretpostavimo sada da Alisa želi da se predstavi Bobu. Prvo, ona na slučajan način bira jedan realan broj i objavljuje $p = r^2$. Zbog činjenice da nalaženje tačnog kvadratnog korjena od p nad poljem $\mathbb{Q}$ samo sa operacijama $\{+, -, *, /\}$ je nemoguće, Alisa je sigurna da samo ona zna r. Mada i sama Alisa ne može biti sigurna da li je r racionalan broj, ona može biti sigurna da samo ona zna r.

Protokol:

1. Alisa bira realan broj s. Daje Bobu $t = s^2$.
2. Bob baca novčić i šalje rezultat Alisi.
3. - Ako Bob kaže "glava", onda Alisa šalje Bobu s
     Bob provjerava da li vrijedi $s^2 = t$.
   - Ako Bob kaže "pismo", onda Alisa šalje Bobu broj $u = r \cdot s$
     Bob provjerava da li vrijedi $u^2 = p \cdot t$.

Ova 3 koraka se ponavljaju nezavisno l puta. Bob će prihvatiti Alisin dokaz identiteta samo ako su sve l provjere bile uspješne[3].

Sada ćemo dokazati da ovakav protokol stvarno jedan protokol identifikacije koji uz svojstva kompletnosti i razumnosti ispunjava i svojstvo zero-knowledge.

Ako Alisa i Bob poštuju protokol, onda Bob uvijek prihvata Alisin dokaz identiteta. Time smo dokazali prvo svojstvo.

Bilo ko ko želi da ukrade Alisin identitet, ne može odgovoriti na oba Bobova pitanja jer on ne može znati i s i rs, jer bi onače mogao lako izračunati r iz $(rs)/s = r$, što se kosi sa činjenicom da on ne može izračunati r ako mu je dato samo polje $\mathbb{Q}$ i r^2. Dakle, u svakoj iteraciji predstavljenog protokola, vjerovatnoća uspjeha napadača je najviše $1/2$. Poslije k iteracija, vjerovatnoća da se Bob može prevariti je najviše 2^{-k}.

Da bismo pokazali da je protokol zero-knowledge, konstruisaćemo jedan simulator koji proizvodi transkripte Bobovog pogleda na prokotol. Bobov pogled je oblika (t, G, s) ili (t, P, u). Prvi pogled može se simulirati slučajnim izborom u i uzimanjem da t bude u^2/p, ako je $u^2/p \leq 1$. Inače, ponovi (izaberi u opet) dok u^2/p nije manje od jedinice. Za očekivati je da će se ovaj proces zaustaviti nakon konačno mnogo iteracija. Ako se izvršavaju k pokušaja u seriji, očekivani broj pokušaja simulatora je $2k$. Ako se paralelno šalju k rezultata bacanja novčića, onda očekivani broj pokušaja je 2^k, što ne predstavlja problem u našem modelu jer nijesmo uveli ograničenja složenosti izračunavanja[4].

[3] t je neki predefinisani sigurnosni parametar.

[4] Ukoliko se uvode ova ograničenja, ostaje otvoreno pitanje da li ovaj protokol ostaje da bude zero-knowledge.

3.4 Primjer protokola autentifikacije

U ovoj sekciji od predstavljenog protokola identifikacije u prethodnoj sekciji, malom modifikacijom, dobićemo zero-knowledge protokol autentifikacije.

Neka je m poruka koju Alisa želi da autentifikuje Bobu. Za ovu svrhu, Alisa generiše na slučajan način dva tajna realna broja $X_{A,1}$ i $X_{A,2}$ i objavljuje $Y_{A_1} = X_{A,1}^2$ i $Y_{A,2} = X_{A,2}^2$. Da bi Bobu potvrdila autentičnost poruke m, Alisa treba dokazati Bobu da zna broj $Z = m \cdot X_{A,1} \cdot X_{A,2}$.

1. Alisa daje Bobu broj $R = K^2$, gdje je K slučajno izabran realan broj.

2. Bob baca novčić i šalje Alisi bit $b = 1$ ako je palo pismo i $b = 0$ ako je rezultat bacanja glava.

3. Alisa šalje Bobu broj $L = K \cdot (m \cdot X_{A,1} \cdot X_{A,2})^b$.
   Bob provjerava da li je $L^2 == R(m^2 \cdot Y_{A,1} \cdot Y_{A,2})^b$.

Analiza protokola. Prvo, ako Eva promijeni poruku m u m', onda će Bob to odmah primjetiti jer se u tom slučaju dobija $L' = K \cdot (m' \cdot X_{A,1} \cdot X_{A,2})^b$ pod pretpostavkom da ona zna još i tajne ključeve.

Bob izaziva Alisu sa dva pitanja, zavisno od rezultata bacanja novčića. Onaj ko zna odgovore na oba pitanja (za $b = 0$ i za $b = 1$) ne može saznati Alisine tajne ključeve niti originalnu poruku. Dalje, primjetimo da svako može efikasno simulirati izvršenje protokoli kojeg čine trojke (L, b, R) iz protokola, tj. ovaj protokol je i zero-knowledge.

3.5 O nemogućnosti enkripcije sa javnim ključem

U prethodne dvije sekcije, vidjeli smo da u ovom modelu moguće kreirati identifikacione protokole i zero-knowledge protokole autentifikacije. U ovoj sekciji, dokazaćemo da šifarski sistemi sa javnim ključem u ovom modelu ne postoje.

Bob hoće Alisi da pošalje poruku m koristeći enkripciju sa javnim ključem, i ova poruka mora ostati tajna za Evu-napadača.

Razmatraćemo nekoliko mogućih scenarija za enkripciju sa javnim ključem. Sa SK označavamo tajni ključ, sa PK javni ključ, sa m otvorenu poruku a sa c njen šifrat. Znanje neke strane u komunikaciji se modelira kao polje koje ta strana može izračunati (generisati).

1. Sistem sa jednim tajnim i jednim javnim ključem.

Alisa počinje sa poljem $\mathbb{Q}$ i zatim bira realan broj SK za njen tajni ključ, čime ona dobija polje $\mathbb{Q}(SK)$. Da bi dobila njen javni ključ PK, ona izvodi neki konačan broj operacija nad poljem $\mathbb{Q}(SK)$. Dakako, $PK \in \mathbb{Q}(SK)$. Zatim, Alisa objavljuje svoj javni ključ PK.

Po objavljivanju javnog ključa, sve strane u komunikaciji (Alisa, Bob i Eva) znaju $\mathbb{Q}(PK)$. Pritom, vrijedi još i $\mathbb{Q}(PK) \subseteq \mathbb{Q}(SK)$.

Neka je $[\mathbb{Q}(SK) : \mathbb{Q}(PK)]$ konačan broj. Bob uzima svoju poruku $m \in \mathbb{R}$ i koristeći se Alisinim javnim ključem generiše šifrat te poruke c. Bob šalje Alisi šifriranu poruku c preko nesigurnog kanala.

Sada Bob vidi: $\mathbb{Q}(PK, m)$ i $\mathbb{Q}(PK, c)$, a Eva vidi $\mathbb{Q}(PK, c)$ (jer je ukrala c a PK je javno dostupan podatak).

Po prijemu broja c, Alisa uzima svoj tajni ključ SK i pomoću neke mašine D računa m. Dakle, Alisa vidi $\mathbb{Q}(PK, c), \mathbb{Q}(SK, c)$ i $\mathbb{Q}(PK, m)$.

Svrha enkripcije je da onemogući da Eva sazna m znajući samo PK i c.

Na osnovu naprijed iznijetog, vrijedi

$$\mathbb{Q}(PK, c) \subseteq \mathbb{Q}(PK, m) \subseteq \mathbb{Q}(SK, c). \qquad (*)$$

Stvarno, $\mathbb{Q}(PK, c) \subseteq \mathbb{Q}(PK, m)$ jer za dato m i PK, enkripter može izračunati c koristeći samo operacije polja, pa je $c \in \mathbb{Q}(PK, m)$. Isto tako, $\mathbb{Q}(PK, m) \subseteq \mathbb{Q}(SK, c)$ je tačno jer za dato c i SK legitimni dekripter (Alisa) može da izračuna otvorenu poruku m, koristeći samo operacije nad poljem.

Analizirajmo sada stepene ovih raširenja. Neka je $n = [\mathbb{Q}(SK) : \mathbb{Q}(PK)]$. Onda, $[\mathbb{Q}(SK, c) : \mathbb{Q}(PK, c)]$ je najviše n jer dodavanjem c poljima $\mathbb{Q}(SK)$ i $\mathbb{Q}(PK)$, može se samo (eventualno) smanjiti stepen minimalnog polinoma elementa SK nad $\mathbb{Q}(PK)$.

TVRDIMO: $\mathbb{Q}(SK, c) = \mathbb{Q}(SK, m)$.

Znamo da $\mathbb{Q}(SK, m) \subseteq \mathbb{Q}(SK, c)$ jer Alisa otvorenu poruku m dobija iz šifrata c koristeći konačno mnogo operacija polja znajući SK. No znajući SK može se lako izračunati i PK jer $\mathbb{Q}(PK) \subseteq \mathbb{Q}(SK)$. Znajući PK i m, bilo ko može lako izračunati c pa je $\mathbb{Q}(SK, c) \subset \mathbb{Q}(SK, m)$. Dakle, $\mathbb{Q}(SK, c) = \mathbb{Q}(SK, m)$.

Dakle, sada imamo $[\mathbb{Q}(SK, c) : \mathbb{Q}(PK, m)] = [\mathbb{Q}(SK, m) : \mathbb{Q}(PK, m)]$. Na osnovu relacija raširenja imamo

$$[\mathbb{Q}(PK, m) : \mathbb{Q}(PK, c)] \cdot [\mathbb{Q}(SK, c) : \mathbb{Q}(PK, m)] = [\mathbb{Q}(SK, c) : \mathbb{Q}(PK, c)].$$

Znamo da je $[\mathbb{Q}(SK, c) : \mathbb{Q}(PK, c)] \leq n$ i $[\mathbb{Q}(SK, c) : \mathbb{Q}(PK, m)] = n$, slijedi da je $[\mathbb{Q}(PK, m) : \mathbb{Q}(PK, c)] = 1$. Iz algebre je poznato da ako je $[K : F] = 1$, onda je $K = F$. Odatle imamo $\mathbb{Q}(PK, m) = \mathbb{Q}(PK, c)$.

Relacija $\mathbb{Q}(PK, m) = \mathbb{Q}(PK, c)$ znači da poruka m pripada i Evinom polju čim ona sazna c. Kako ona ima neograničeno vrijeme računanja i kako je $\mathbb{Q}(PK, c)$ prebrojivo, Eva prebrojava sve elemente tog polja i upotrebnom mašine enkripcije (koja je javno dostupna) nad svakim tim elementom, koristeći PK provjerava da li dobijeni rezultat jednak c. Ukoliko jeste, to znači da je dobila poruku m, a inače, nastavlja sa sljedećim.

2. Sistem sa više javnih ključeva i više tajnih ključeva.

Sada razmotramo slučaj kada Alisa umjesto jednog tajnog ključa koristi n tajnih ključeva i l javnih ključeva i pitamo se da li je sada enkripcija sa javnim ključem moguća.

Označimo tajne ključeve redom sa $SK_1, SK_2, \ldots, SK_n$ i javne ključeve sa $PK_1, PK_2, \ldots, PK_l$ redom. Kako sve strane u komunikaciji mogu da izvode samo konačan broj operacija, može se generisati samo konačan broj javnih i tajnih ključeva.

Ako je svaki tajni ključ SK_i algebarski nad poljem $\mathbb{Q}(PK_1, \ldots, PK_m)$, onda će $[\mathbb{Q}(SK_1, \ldots, SK_n) : \mathbb{Q}(PK_1, \ldots, PK_m)]$ biti konačan broj. Koristeći prednje, opet zaključujemo da je enkripcija nemoguća i u ovom scenariju.

3. Vjerovatnosna enkripcija.[5]

U prethodnim sistemima enkripcije, enkripter je tokom enkripcije mogao sprovesti samo operacije nad poljem. Sada ćemo mu omogućiti da bira realne brojeve. Time su dakle Eva i Bob dobili mogućnost da biraju realne brojeve. Za trenutak, pretpostavimo da je stepen polja legitimnog dekriptera (Boba) nad Evinim konačno. Razmotrimo slučaj jednog tajnog i jednog javnog ključa.

Da li je ovime Eva dobila na snazi?

Odgovor je negativan. Enkripter poruke radi sa poljem $\mathbb{Q}(PK, m, r_1, \ldots, r_m)$, gdje je r_i slučajno izabran realan broj. Eva sada može imati polje $\mathbb{Q}(PK, c) \subset \mathbb{Q}(PK, m, r_1, \ldots, r_m)$. Da bi Eva saznala nešto o poruci izborom realnih brojeva, ona mora koristeći tu operaciju i operacije polja da generiše element iz $\mathbb{Q}(PK, m, r_1, r_2, \ldots, r_m) \setminus \mathbb{Q}(PK, c)$. Pretpostavimo da je Eva na slučajan način izabrala l realnih brojeva $s_1, \ldots, s_l$. Onda, ona ima polje $\mathbb{Q}(PK, c, s_1, \ldots, s_l)$. Svaki element ovog polja ima oblik $p(PK, c, s_1, \ldots, s_l)$ $/q(PK, c, s_1, \ldots, s_l)$, pri čemu su p i q polinomi sa racionalnim koeficijentima sa nepoznatim $PK, c, s_1, \ldots, s_l$. Da bi generisala element y iz $\mathbb{Q}(PK, m, r_1, \ldots, r_l) \setminus \mathbb{Q}(PK, c)$, moramo imati neki izraz oblika

$$y = p(PK, c, s_1, \ldots, s_l)/q(PK, c, s_1, \ldots, s_l).$$

Znamo da p/q nije u $\mathbb{Q}(PK, c)$, obzirom da smo pretpostavili da y nije u $\mathbb{Q}(PK, c)$. Bitno je uočiti da nisu svi koeficijenti s_i u izrazu p/q nulti, i da se ne svi koeficijenti s_i u p skraćuju sa koeficijentima u q (tj. nema skraćivanja tipa $(s_1 + s_2)/3(s_1 + s_2) = 1/3$). U tom slučaju, p/q bi zapravo bio element $\mathbb{Q}(PK, c)$. Ali, time je ustanovljena netrivijalna relacija među s_i ovima nad poljem $\mathbb{Q}(PK, c)$. Ako je s_i slučajni realni broj, vjerovatnoća ove pojave je 0, obzirom da je polje $\mathbb{Q}(PK, c)$ skup mjere nula na skupu $\mathbb{R}$. Zaključujemo, da slučajnim izborom realnih brojeva, napadač - Eva, ne dobija na snazi.

Dozvolimo sada enkripteru da probabilisticki šifrira neku poruku, tj. dajemo mu mogućnost izbora slučajnih realnih brojeva. I dalje, imamo sljedeći niz polja:

$$\mathbb{Q}(PK, c) \subseteq \mathbb{Q}(PK, m) \subseteq \mathbb{Q}(SK, c),$$

[5] U klasičnoj enkripciji, za više ponavljanja procesa enkripcije nad porukom m dobija se isti šifrat c, tj. za više ponavljanja procesa enkripcije $c = \mathcal{E}(m, PK)$ se ne mjenja. Ovo sistem čini podložnim za napad, pa je sredinom osamdesetih, uvedena takozvana vjerovatnosna enkripcija, u kojem se tokom procesa enkripcije upotrebljavaju slučajni brojevi kako bi se sprečio pomenuti napad.

pri čemu, da bi shema enkripcije bila sigurna, sve relacije inkluzije moraju biti stroge. Međutim, polje enkriptera nije više $\mathbb{Q}(PK, m)$, već $\mathbb{Q}(PK, m, r_1, \ldots, r_m)$, gdje su $r_1, \ldots, r_m$ slučajno izabrani realni brojevi. Međutim, primjenom prethodno ukazanih argumenata dobijamo opet da inkluzije u tornju ne mogu biti stroge, odnosno $\mathbb{Q}(PK, c) = \mathbb{Q}(PK, m)$. Time, iako Eva ne može da restaurira Bobovo originalno polje $\mathbb{Q}(PK, m, r_1, \ldots, r_m)$, ona može generisati $\mathbb{Q}(PK, m)$ a time, listanjem svih članova tog polja i provjerom da li za neki element x tog polja vrijedi $c = \mathcal{E}(x, PK)$ dobiti poruku m.

4. Slučaj kada $[\mathbb{Q}(SK) : \mathbb{Q}(PK)]$ nije konačno.

Razmotrimo sada slučaj kada Alisa generiše realne brojeve r, s da joj budu njen tajni ključ, a broj rs proglašava za javnim ključem. To je dakle slučaj kada je $[\mathbb{Q}(SK) : \mathbb{Q}(PK)]$ beskonačan. U ovom slučaju, $\mathbb{Q}(rs) \subseteq \mathbb{Q}(r, s)$, ali je sada $[\mathbb{Q}(SK) : \mathbb{Q}(PK)] = \infty$, a mi želimo da nam inkluzije $\mathbb{Q}(PK, c) \subseteq \mathbb{Q}(PK, m) \subseteq \mathbb{Q}(SK, c)$ budu stroge. Paradigma enkripcije sa javnim ključem predviđa mogućnost da se šifrat c iz poruke m dobija pomoću neke mašine upotrebom brojeva r i s, i obratno, da se m uspješno može izračunati iz c pomoću broja rs. Međutim, situacija je ovdje problematična u smislu što imamo nepreprebrojivo mnogo šifrata jedne te iste poruke. Kako se svaki element y koji je algebarski nad $\mathbb{Q}(SK)$ nalazi i u algebarskom zatvorenju $\mathbb{Q}(SK)$, i kako je algebarsko zatvorenje od $\mathbb{Q}(SK)$ prebrojivo, vjerovatnoća da će šifrat biti algebarski nad $\mathbb{Q}(SK)$ je 0. Dakle, c je transcendentan nad $\mathbb{Q}(SK)$ sa vjerovatnoćom 1.

Sada, kako je c transcendentan nad $\mathbb{Q}(SK)$ (a time i nad $\mathbb{Q}(PK)$), međupolja polja $\mathbb{Q}(SK, c)/\mathbb{Q}(PK, c)$ su oblika $L(c)$, pri čemu je L neko međupolje od $\mathbb{Q}(SK)/\mathbb{Q}(PK)$.

Podsjedtimo se Luroth-ove teoreme koja tvrdi: ako je a transcendentan nad poljem F, onda svako međupolje L polja F i $F(a)$ ima oblik $L = F(u)$, pri čemu je u oblika $\frac{p(x)}{q(x)}$, gdje su p i q polinomi nad F. Na osnovu ove teoreme, sva međupolja polja $\mathbb{Q}(SK)/\mathbb{Q}(PK)$ imaju oblik $\mathbb{Q}(u)$, pri čemu je u broj oblika $p(SK)/q(SK)$, gdje su p i q dva polinoma sa koeficijentima nad $\mathbb{Q}$ i nepoznatim nad SK, i pri čemu važi još da je $q \neq 0$. Da bi željene inkluzije bile prave, $\mathbb{Q}(PK, m)$ mora biti oblika $\mathbb{Q}(u, c)$. Međutim, rekli smo da je u broj oblika $p(SK)/q(SK)$ i pritom $u \notin \mathbb{Q}(PK, c)$, a takav broj je nemoguće generisati znajući samo PK i m (koji su uz to i algebarski i nezavisni od SK). Štaviše, vjerovatnoća da se takav broj može generisati čak ako je dozvoljeno da se generišu realni brojevi. Dakle, polje $\mathbb{Q}(PK, m)$ ne sadrži elemente oblika $p(SK)/q(SK)$, pa time smo dobili smo da je $\mathbb{Q}(PK, m) = \mathbb{Q}(PK, c)$.

Dakle, ovim smo dokazali, da u našem modelu izračunljivosti, nije moguće ispostaviti sistem enkripcije sa javnim ključem.

3.6 Neke napomene

Sada dajemo par napomena o tumačenju prednjih rezultata i objašnjenja o nekim pretpostavkama kada smo vršili modifikacije nad osnovnim BSS modelom i zašto pretpostavljamo da sve strane u komunikaciji imaju neograničene resurse računanja.

Napomena 3.6.1 *U kriptografiji se ne govori o nemogućnosti razbijanja nekog kriptosistema, već o "malim šansama da se to izvede za neko razumno vrijeme". Isto tako, često se u literaturi navodi da su računarski resursi strana ograničena na neki "razuman" način. BSS mašine su moćne (čak neuporedivo moćnije u odnosu na Turingov model). Nad $\mathbb{R}$ i nad $\mathbb{C}$ aritmetičke operacije brojeva bilo koje veličine se izvode u jednom koraku. Zato recimo polinomijalne mašine nad $\mathbb{R}$ ili nad $\mathbb{C}$ mogu da rješavaju teške diskretne probleme varanjem na sljedeći način: brzo kodira neku eksponencijalnu količinu informacija kao velike brojeve i dobijanjem eksponencijalne količine esencijalnih bit operacija koje su urađene za par koraka. Zbog ovoga, mi smo ovdje "razumno" ograničili računske resurse tako što su sve strane ograničene na izvođenje samo operacija nad poljem i računati samo racionalne funkcije. Time je dobijen jedan neuporedivi slabiji model u odnosu na puni BSS model. Ali, da bismo kompenzirali uvedeno slabljenje, svim stranama je dozvoljeno da izvrše neograničeno ali konačno mnogo računskih operacija. Time je zapravo, na pravi način modeliran jedno algebarsko okruženje računanja sa radikalima.*

Napomena 3.6.2 *Sheme enkripcije sa javnim ključem se po pravilu konstruišu iz takozvanih jednosmjernih funkcija sa tajnim prolazom, tj. funkcija koje se se lako računaju i bez znanja neke dodatne lozinke (tajnog prolaza) teško invertuju, a inače, lako.*

Pokazuje se (vidi [8]) da je sigurna enkripcija sa javnim ključem u Turingovom modelu moguća ako je data jednosmjerna funkcija sa tajnim prolazom. Mi smo u ovom poglavlju pokazali da je ista nemoguća i time potragu za jednosmjernim funkcijama sa tajnim prolazom na našem modelu (gdje svaka strana može sprovesti neograničeno ali konačno mnogo računskih koraka) čini izlišnom.

3.7 Zaključak

Pokazali smo da u predstavljenom modelu izračunljivosti, gdje sve strane u komunikaciji (legalni enkripteri i napadač) imaju neograničenu ali konačnu snagu računanja nad poljem $\mathbb{Q}$, enkripcija sa javnim ključem je nemoguća. Ali, zato pokazali smo da zero-knowledge protokoli identifikacije i autentifikacije postoje.

Prostor znanja, tj. prostor informacija do kojih strane u komunikaciji mogu doći je modeliran kao polje koje ta strana može izračunati koristeći neograničeno ali konačno mnogo operacija polja. Pokazali smo da u ovom modelu napadač može lako izračunati originalnu poruku znajući samo javni ključ, tj. da je $\mathbb{Q}(PK, m) = \mathbb{Q}(PK, c)$, pri čemu su PK, m i c redom javni ključ, originalna poruka i šifrirana poruka.

Poglavlje 4

Kriptografija u pitagorejskoj BSS mašini

U ovom poglavlju razmatramo problem kriptografije pomoću lenjira i šestara. Prvo ćemo na adekvatan način modelirati operacije lenjirom i šestarom u algebarskom okruženju, a zatim, kao i u osnovnom modelu iz poglavlja 4, pokazaćemo da zero-knowledge identifikacija i autentifikacija su ostvarljive. Zatim dokazujemo da i u ovom modelu se ne može uspostaviti sigurna shema enkripcije sa javnim ključem.

Obzirom da razmatramo kriptografske primitive u okruženju koju su uspostavili grčki matematičari, u ovom poglavlju ćemo umjesto imena Alisa, Bob i Eva – za legalne enkriptere i napadača, koristiti nazive Arhimed, Euklid i rimljanin iako oni nijesu bili savremenici[1].

4.1 Konstrukcije pomoću lenjira i šestara

Neka je OA jedinična duž u kompleksnoj ravni $\mathbb{C}$, određena tačkama $O(0,0)$ i $A(0,1)$. Tačka $M(x,y) \in \mathbb{C}$ je *konstruktivna* ako se može dobiti elementarnom konstrukcijom pomoću lenjira i šestara u konačno mnogo koraka, polazeći od duži OA. Preciznije, konstruktivne tačke, duži, prave i kružnice uvode se pomoću sljedećih aksioma:

A1. Tačke O, A su konstruktivne.

[1] Arhimed je rođen oko 287. godine pne., a umro je 212. ili 211. godine pne. Za Euklida se zna da je rođen 325. godine pne i da je umro 265. godine pne. Pitagora je živio još ranije oko 571 – 496 pne. Dakle, ovi matematičari nijesu bili savremenici.

A2. Ako su B i C konstruktivne tačke i $B \neq C$, onda je prava (duž) određena tačkama B i C konstruktivna.

A3. Kružnica koja ima konstruktivan centar i konstruktivan poluprečnik je konstruktivna.

A4. Presjek dvije konstruktivne prave je konstruktivna tačka.

A5. Presjeci dvije konstruktivne kružnice su konstruktivne tačke.

A6. Presjeci konstruktivne kružnice i konstruktivne prave su konstruktivne tačke.

Skup kontruktivnih tačaka $\mathcal{P}$ u $\mathbb{C}$ naziva se *pitagorejska ravan.* Ako je $M(x, y) \in \mathcal{P}$, tada se x i y nazivaju konstruktivnim realnim brojevima.

Neposredno se provjerava da je $\mathcal{P}$ prebrojiv skup.

Teorema 4.1.1 *Neka je $\mathcal{K}_R$ skup svih konstruktivnih realnih brojeva. Tada*

1. *$\mathcal{K}_R$ je potpolje polja $\mathbb{R}$.*
2. *$\mathcal{P}$ je potpolje polja $\mathbb{C}$.*
3. *$\mathcal{K}_R \subseteq \mathcal{P} \subseteq \mathbf{A}$, gdje je $\mathbf{A}$ polje algebarskih brojeva.*

Neka je $r \in \mathcal{K}_R$ dobijen elementarnom konstrukcijom u jednom koraku, tj. pomoću aksioma A1-A6 iz tačaka koje pripadaju polju $\mathbf{F}$. Tada je r rješenje sistema linearnih jednačina ili neke kvadratne jednačine, pa vrijedi: $[F(x) : F] \in \{1, 2\}$. Otuda, ako je $r \in \mathcal{K}_R$, tada postoji neko $n \in \mathbf{N}$ td. $[\mathbb{Q}(r) : Q] = 2^n$. Stvarno, ako je $\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq ... \subseteq F_m$ niz polja koja prati elementarnu konstrukciju broja $r \in F_m$, tada

$$[F_m : \mathbb{Q}] = [F_m : F_{m-1}] \ldots [F_1 : F_0] = 1 \cdot 2 \cdot 1 \cdot 2 \cdot 2 \cdot 1 \cdot \ldots \cdot 1 = 2^n.$$

Podsjetimo se sada Delskih problema:

1. **Problem kvadrature kruga**: Konstruisati kvadrat koji ima površinu jednaku površini kruga poluprečnika 1.
   Konstrukcija nije moguća jer je π transcendentan broj, te rješenje jednačine $x^2 = \pi$ nije algebarski.

2. **Problem udvostručavanja kocke.** Konstruisati kocku dvostruko veće zapremine od jedinične kocke.
   Konstrukcija nije moguća jer $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^n$ za neko $n \in \mathbf{N}$, pri čemu je $\sqrt[3]{2}$ dužine ivice udvostručene kocke.

3. **Problem trisekcije ugla.** Podijeliti ugao na tri jednaka dijela.
   Konstrukcija nije moguća. Za $\alpha = 60$, ugao $\beta = 20$ nije konstruktivan jer bi u tom slučaju i $\cos 20$ bio konstruktivan. Naime, kako je $\cos 2\theta = 4\cos^3\theta - 3\cos\theta$, tada bi $\cos 20$ zadovoljavao jednačinu $4x^3 - 3x - 1/2 = 0$, a polinom $4x^3 - 3x - 1/2$ je nesvodljiv nad $\mathbb{Q}$ jer nema racionalnih korjena. Dakle, $[\mathbb{Q}(\cos 20) : \mathbb{Q}] = 3 \neq 2^n$ za neko $n \in \mathbf{N}$, pa $\cos 20 \notin \mathcal{K}_R$.

4.2 Opis pitagorejske BSS mašine

Označimo sa G skup svih konstruktivnih pravih a sa K skup svih konstruktivnih krugova. Ako su $Q, Q', Q'' \in \mathcal{P}, Q' \neq Q"$, onda parom (Q', Q'') u potpunosti je određen jedna duž i prava u kojoj ta duž leži. Sa $(Q; Q', Q'')$ potpuno je određena kružnica sa centrom u Q i poluprečnikom koji je određen segmentom (Q', Q'').

Naš cilj je da operacije lenjirom i šestarom modeliramo algebarskim mašinama, odnosno da geometrijske probleme prevodimo u algebarske.

Ako su q_i i q_j dvije prave (duži), onda presjek $q_i \cap q_j$ jeste: jedna tačka (ako se one sijeku), nijedna tačka (ako su mimoilazne) ili beskonačno mnogo (ako se poklapaju). Ovu operaciju možemo modelirati rješenjem sistema

$$\begin{aligned} a_1x + a_2y &= c_1 \\ b_1x + b_2y &= c_2. \end{aligned}$$

Ako je k_j neka kružnica i q_i neka prava, onda je njihov presjek $p_k = q_i \cap k_j = k_j \cap q_i$ tačka (nijedna, jedna ili dvije) koja se algebarski dobija rješavanjem sistema

$$\begin{aligned} a_1x + a_2y &= c_1 \\ (x - b_1)^2 + (y - b_2)^2 &= c_2^2. \end{aligned}$$

Slično, presječne tačke dva kruga nalaze se rješavanjem sistema

$$(x - a_1)^2 + (y - a_2)^2 = c_1^2$$
$$(x - b_1)^2 + (y - b_2)^2 = c_2^2.$$

U kriptografiji neophodna je mogućnost da se generišu i čuvaju neki "slučajni" objekti koje se ne mogu iskonstruisati pomoću lenjira i šestara u konačno mnogo koraka, jer inače bi napadač mogao da ih sazna. Slično se i u geometriji često pribjegava generisanjem neke slučajne veličine – recimo kada se u procesu nalaženja raspolovice duži "šestar otvara proizvoljno više od polovine".

Zbog prednjeg, pretpostavljamo da sve strane u komunikaciji mogu da izaberu na slučajan način, ravnomjerno raspodjeljenu tačku unutar jediničnog kruga i da mogu da bacaju novčić.

U terminima Blum, Shub i Smale modela, radimo sa vjerovatnosnom mašinom nad poljem $\mathbb{C}$, koja može generisati slučajne kompleksne brojeve. Tokom računanja radimo sa poljem $\mathbb{K} = \mathbb{Q}[i] = \{p + qi | p, q \in \mathbb{Q}\}$ koja je jedno potpolje polja $\mathbb{C}$ i jedno raširenje polja $\mathbb{Q}$. Ovu mašinu nazvaćemo *pitagorejskom BSS mašinom* a odgovarajući model izračunljivosti *pitagorejski model izračunljivosti*. Najveći stepen polinoma u ovoj mašini je 2, pa je i stepen ove mašine 2.

4.3 O izračunljivosti u pitagorejskom modelu

Moć izračunavanja u pitagorejskom modelu je ograničen. Prva pomisao bi bila da su u ovom modelu sve funkcije sa korjenima izračunljive jer je korjenovanje izvodljivo pomoću lenjira i šestara. Međutim, to u ovom modelu nije tačno zato što čvorovi grananja rade sa operacijom "=" i zbog toga nema načina kako da se kontrolišu slučajevi kada bi mašina ušla u neko neregularno stanje. Algebarskim jezikom rečeno, nemamo načina da ispitamo kada je neka diskrimanta pozitivna kako bismo na ispravan način odlučili o rješenjima pomenutih sistema jednačina. Zato, klasu izračunljivih funkcija u ovom okruženju čine racionalne funkcije. U daljem tekstu ćemo operacije pomoću lenjira i šestara koje odgovaraju pitagorejskom modelu (tj. sve operacije bez operacije korjenovanja) nazvati redukovane operacije pomoću lenjira i šestara.

4.4 Jednosmjerne funkcije

Kao što smo naveli u uvodnoj sekciji ovog poglavlja, funkcija $f(X) = 3X$ se lako računa. Invertovanje ove funkcije – trisekcija ugla je nemoguća ako X nije u nekom raširenju polja $\mathbb{Q}$ sa radikalima. Stvarno, ugao $Y = f(X)$ se može podijeliti u 3 jednaka dijela pomoću lenjira i šestara ako jednačina $\cos Y = 4x^3 - 3x$ ima rješenje u nekom raširenju polja $\mathbb{Q}(\cos Y)$ sa radikalima. Slijedi da je $\cos Y$ algebarski i skup svih uglova koji se mogu podijeliti u tri jednaka dijela je jedan skup mjere nula. Dakle, za skoro sve uglove Y trisekcija nije moguća pa je $f(X) = 3X$ stvarno jedna jednosmjerna funkcija.

Dakle, i u ovom modelu jednosmjerne funkcije postoje.

Napomena 4.4.1 *U članku [7] senzacionalno se objavljuje da je jedna matematičarka otkrila način kako da se izvrši trisekcija ugla i tvrdi da je time opovrgla čitavu teoriju Galois. Pažljivom analizom tog članka dolazi se do zaključka da se zapravo radi o jednom aproksimativnom algoritmu za trisekciju ugla. Štaviše, radi se o jednom brzo konvergirajućem algoritmu koji u 4 koraka nalazi vrlo dobru aproksimaciju trećine nekog ugla. Postavlja se pitanje da li je time ugrožen naš kriptografski model? Odgovor je negativan, zato što u pitagorejskom mašinu, u svakoj ćeliji se čuva jedan kompleksan broj sa beskonačnom tačnošću (mada to može čak zvučati previše idealno) i u ovom modelu ne govorimo i ne radimo sa aproksimativnim vrijednostima.*

4.5 Identifikacioni protokol

Koristeći jednosmjernu funkciju $f(X) = 3X$ definisaćemo jedan zero-knowledge protokol identifikacije.

Razmatraćemo situaciju kada Hipasus[2] na ulazu u pitagorejski kamp mora da ubijedi čuvara da je to stvarno on.

Inicijalizacija. Prilikom prijema u ovo elitno društvo, svaki član pa i Hipasus u matičnu knjigu škole ostavlja neki ugao Y_H koji je dobijen utrostručavanjem nekog slučajno izabranog ugla. Zbog toga što je trisekcija pomoću

[2]Hipasus – pripadnik pitagorejske škole, prvi je matematičar koji je otkrio iracionalne brojeve. Koristeći teoremu svog učitelja – Pitagore, on je dobio broj koji se nije mogao predstaviti pomoću dva cijela broja. Pitagora ne samo da se nije ubijedio u korektnost Hipasusovog izlaganja, već se toliko naljutio da je Hipasusa osudio izbacivanjem iz škole.

lenjira i šestara nemoguća, Hipasus može biti siguran da jedino on zna originalni ugao X_H.

Protokol.

1. Hipasus daje čuvaru kopiju nekog ugla R koji je dobijen utrostručavanjem slučajno izabranog ugla K.

2. Čuvar baca novčić o saopštava Hipasusu rezultat.

3. Ako čuvar kaže "Glava", onda Hipasus daje čuvaru kopiju ugla K i čuvar provjerava da li je $3K = R$.
   Ako čuvar kaže "Pismo", Hipasus daje kopiju ugla $L = K + X_H$ i čuvar na osnovu podataka iz matične knjige provjerava da li je $3L = R + Y_H$.

Ova 3 koraka se ponavljaju t puta nezavisno, pri čemu je t neki predefinisani sigurnostni parametar. Čuvar prihvata Hipasusov dokaz identiteta samo ako su sve t provjere bile uspješne.

Ovaj protokol jeste jedan interaktivan zero-knowledge identifikacioni protokol.

Stvarno, čuvar će uvijek prihvatiti Hipasusov dokaz identiteta. Međutim, neki prevarant koji nezna tajni ugao X_H ne može konstruisati oba ugla K i L u koraku 3. Zato, čuvar će sa vjerovatnoćom najviše $1/2$ za bilo koju seriju ponavljanju i sa vjerovatnoćom 2^{-t} za sva t ponavljanja prihvatiti Hipasusov dokaz identiteta.

Simulirajmo sada čuvarev pogled tokom izvršavanja protokola. Čuvar "vidi" Hipasusove poruke i zna rezultate svog bacanja novčića što se može predstaviti kao $(R, "Pismo", K)$ ili $(R, "Glava", L)$. Da bi čuvar simulirao ove transkripte, uzima ugao K na slučajan način i računa $R = 3K$, čime smo simulirali prvu trojku. Za drugu, bira ugao L na slučajan način i rješava $3L = R + Y_H$ po R. Dakle, čuvar može simulirati ovu interakciju sa Hipasusom i neće dobiti nikakvo znanje o njegovom tajnom uglu X_H. Dakle, ovaj protokol ima zero-knowledge svojstvo.

Paralelizacija. Razmotrimo slučaj kada i Hipasus i čuvar mogu da rade više operacija istovremeno. Za ovakav protokol istovremeno se izvršavaju t iteracije protokola:

1. Hipasus daje čuvaru t kopija uglova R_i.

2. Čuvar baca t novčića i daje Hipasusu odgovore u vidu neke n-torke nula i jedinica.

3. Hipasus daje čuvaru t kopija odgovarajućih uglova L_i ili R_i

Tokom napada ovog protokola, očekivani broj pokušaja simulacije je 2^t i obzirom da nijesu uvedena ograničenja broja mogućih iteracija konstrukcije tokom simulacije su izvodljive. Dakle, i paralelna verzija protokola je zero-knowledge.

4.6 Nemogućnost enkripcije sa javnim ključem

Razmatramo situaciju kada Arhimed želi da Euklidu pošalje neku tajnu poruku koju će kodirati pomoću duži i uglova. Recimo, slovo Δ se kodira pomoću tri duži, odnosno pomoću 6 tačaka pitagorejske ravni. Slično, slovo Φ se kodira pomoću jedne kružnice (3 tačke) i jedne duži (2 tačke) odnosno sa ukupno 5 tačaka. Znak blanko se kodira pomoću donje crte tj. sa parom (0,0) i (1,0). Ovakvim postupkom, možemo dobiti jedno optimalno kodiranje grčkih slova pomoću n-torke tačaka kompleksne ravni.

Pretpostavimo da jednu veliku tekstualnu poruku šifriramo znak po znak, odnosno tačku po tačku. Dakle, u daljem tekstu smatraćemo da Arhimed želi Euklidu poslati jednu tačku $M(x, y)$. Stanje znanja strane u komunikaciji, kao i u poglavlju 3, smatramo poljem koju ta strana može izračunati koristeći osnovne operacije nad poljem.

Euklid je prije početka komunikacije izabrao neku tačku $SK_\Pi = (SK_x, SK_y)$. Ta tačka će biti njegov tajni ključ. Polje koje on zna u ovom trenutku je $\mathbb{K}(SK_x, SK_y)$, pri čemu je $\mathbb{K} = \mathbb{Q}[i]$. Zatim, pomoću neke pitagorejske mašine (odnosno pomoću nekog niza redukovanih operacija pomoću lenjira i šestara) računa javni ključ $PK_\Pi = (PK_x, PK_y) \in \mathbb{K}(SK_x, SK_y)$ i objavljuje ga. Radi kraćeg pisanja, pisaćemo $\mathbb{K}(SK)$ umjesto $\mathbb{K}(SK_x, SK_y)$ i $\mathbb{K}(PK)$ umjesto $\mathbb{K}(PK_x, PK_y)$.

Arhimed sada uzima Euklidov javni ključ PK_Π i poruku $M(x, y)$ i pomoću neke pitagorejske mašine računa njen šifrat $C = (x_c, y_c)$. Zatim, Arhimed po nekom kuriru, šalje Euklidu šifrovanu poruku C. Cilj je da Rimljani ni u kom slučaju ne budu u stanju da izračunaju $M = (x, y)$.

Primjenjujući razmatranja iz sekcije 3.5 nad poljem $\mathbb{K}$, doći ćemo do zaključka $\mathbb{K}(PK, C) = \mathbb{K}(SK, C) = \mathbb{K}(PK, M)$. Ovdje posebno dolazi do izražaja slučaj sa više ključeva jer $PK = (PK_x, PK_y)$ i $SK = (SK_x, SK_y)$.

Dakako, slučaj $[\mathbb{K}(SK) : \mathbb{K}(PK)] = \infty$ ovdje otpada. Operacije pitagorejske mašine proizvode raširenja stepena 1 ili 2.

Kako Rimljani nalaze M iz C znajući $\mathbb{K}(PK, C) = \mathbb{K}(SK, C) = \mathbb{K}(PK, M)$? Rimljani listaju sve tačke $X \in \mathbb{K}(PK, C)$ i mašinom/postupkom za enkripciju (koja je javno dostupna) koristeći PK_Π i X dobijaju neki šifrat C_X od tačke X. Zatim, provjeravaju da li je $C = C_X$. Ako jeste, onda je $M = X$. Inače, ponavljaju postupak za sljedeću tačku.

Napomena 4.6.1 *Može izgledati čudno da je gornji postupak izvodljiv i da je on razlog da smo enkripciju u ovom modelu proglasili nesigurnom. Proces traženja M iz polja $\mathbb{K}(PK, C)$ prebrojavanjem može biti mukotrpan proces, ali on jeste efikasan. Sigurnosni zahtjevi u kriptografiji su takvi da se traže male šanse da napadač restaurira podatak M bez ikakvih pretpostavki o obliku i kvantitavnih osobinama te tačke. Tako recimo tačka* $(74744780998, \frac{8982374391}{329874238987234} \cdot 10^{5983944})$ *koja se dobija poslije velikog broja iteracija ima isti tretman kao i tačka* $M = (1, \frac{1}{2})$ *koja se dobija poslije par koraka.*

Poglavlje 5

Zaključci i otvorena pitanja

Tradicionalno, računarstvo se razvijalo i bavilo prevashodno izračunavanjima nad prstenom cijelih brojeva. Pojava Blum, Shub & Smale modela dala je veliki podsticaj razmišljanjima da se teorija računarstva proširi i bavi i realnim i kompleksnim brojevima. Po pojavi ovog modela, i drugi uvedeni modeli koji su tretirali izračunljivost nad $\mathbb{R}$ su dobili na značaju, posebno *Type Two Effectivity Model* i Valiantov model.

U ovom radu, predstavili smo mogućnost razvoja kriptografije u jednom slabom BSS modelu izračunljivosti i pokazali dometi ostvarljivosti te ideje. U cilju dobijanja odgovora da li je moguće na siguran način šifrirati realne brojeve, ostaje otvoreno pitanje postojanja kriptografskih primitiva u TTE modelu i na Valiantovom modelu izračunljivosti.

Pokazali smo da u ovom modelu jednosmjerne funkcije postoje i da je zero-knowledge identifikacija i autentifikacija moguća. Nažalost, u tim okolnostima nije moguće definisati sistem enkripcije sa javim ključem. U petom poglavlju smo u duhu Dekartovog koordinatnog sistema, geometrijske probleme i operacije pomoću lenjira i šestara predstavili u algebarskom okruženju i dobili sličan model kao nad $\mathbb{Q}$ na kojem važe isti rezultati kao u poglavlju 3.

U sekciji 3.2. predstavili smo zero-knowledge identifikacioni protokol. Ostaje otvoreno pitanje da li taj protokol ostaje da bude zero-knowledge ako se uvode neka ograničenja u računskim resursima.

U četvrtom poglavlju opisali smo model koji ne obuhvata sve izvodljive operacija pomoću lenjira i šestara. Jedan od načina da se definiše potpuni

algebarski model koji će potpuno opisati operacije lenjirom i šestarom jeste da se u mašini ugradi neka crna kutija koja računa apsolutnu vrijednost. Time ćemo omogućiti upoređivanje veličina i omogućiti odlučivanje da li je neki realan broj pozitivan ili ne, tako što će se provjeriti da li važi $a \cdot |a| = a^2$. Znajući da li je jedan broj pozitivan ili ne, nećemo imati neregularna stanja u slučaju pokušaja da se traži kvadratni korjen nekog negativnog broja. Ovim mašinama modeliraju se sve operacije lenjirom i šestarom i dobijen je jedan novi model čija je klasa izračunljivih funkcija šira od klase mašina opisanih u ovom radu. Ostaje otvoreno pitanje da li je u ovom modelu moguće definisati sigurnu shemu enkripcije sa javnim ključem. Naša slutnja je da i u ovom modelu vrijede isti rezultati kao u modelima koji su razmatrani u ovom radu.

Literatura

[1] DAVID P. WOODRUFF, MARTEN VAN DIJK, *Cryptography in an Unbounded Computational Model.* EUROCRYPT 2002: 149-164

[2] L. BLUM, F. CUCKER, M. SHUB, S. SMALE, *Complexity and Real Computation*, Springer, 1997.

[3] M. BURMESTER, R. RIVEST, A. SHAMIR, *Geometric Cryptography: Identification by Angle Trisection*, 4.11.1997, elektronski dokument.

[4] N. BOŽOVIĆ, Ž. MIJAJLOVIĆ, *Uvod u teoriju grupa.* Naučna knjiga Beograd, Treće izdanje 1990.

[5] O. GOLDREICH, *Foundations of Cryptography, Volume I Basic Tools.* Cambridge Preš, 2003.

[6] PASCAL KOIRAN, *A Weak Version of the Blum, Shub & Smale Model.* NeuroCOLT Technical Report Series NC-TR-94-5, August 1994.

[7] Rešenje "nerešivog", Magazin (nedjeljni dodatak uz dnevni list Politika) 30.06.2002. godine, str. 20.

[8] SH. GOLDWASSER, M. BELLARE, *Lecture Notes on Cryptography*, elektronski dokument, August 2001.

[9] S. LANG, *Algebra*, Third Edition, Addison-Wesley, 1999.