Identifikacijske sheme i osobna autentikacija

Ugrica, Bojan

Master's thesis / Diplomski rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:829878

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-20**

Repository / Repozitorij:

Repository of School of Applied Mathematics and Computer Science

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike i računarstva

Bojan Ugrica

Identifikacijske sheme i osobna autentikacija

Diplomski rad

Osijek, *2017.*

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike i računarstva

Bojan Ugrica

Identifikacijske sheme i osobna autentikacija

Diplomski rad

Mentor:
izv. prof. dr. sc. Ivan Matić

Osijek, *2017.*

Sadržaj

1 Uvod **1**

2 Izazov-i-odgovor i postavke tajnoga ključa **4**

3 Model napada i protivnički ciljevi **9**
3.1 Međusobna provjera autentičnosti 10

4 Izazov-i-odgovor u postavkama javnog ključa **14**
4.1 Certifikati 14
4.2 Identifikacijske sheme javnoga ključa 15

5 Schnorrova identifikacijska shema **18**
5.1 Sigurnost Schnorrove identifikacijske sheme 21

6 Okamotova identifikacijska shema **26**

7 Guillou-Quisquaterova identifikacijska shema **31**
7.1 Identifikacijske sheme bazirane na identiteti 34

8 Literatura **35**

9 Sažetak **36**

10 Title and summary **37**

11 Životopis **38**

1 Uvod

Tema ovog rada je identifikacija, koja je također poznata kao Osobna autentikacija. Grubo rečeno cilj identifikacijske sheme je potvrditi nečiji identitet. Obično je to odrađeno u "real time" vremenu. Kriptografski alati kao što je potpisna shema (signature schemes) dozvoljavaju autentikaciju podataka, što može biti odrađeno u bilo kojem trenutku nakon što je bitna poruka (relevant message) potpisana. Pretpostavimo da želimo potvrditi svoj identitet nekome drugome. Ponekad je rečeno da se to može učiniti na jedan od tri načina: na temelju onoga što si, na temelju onoga što posjeduješ ili na temelju onoga što znaš. "Na temelju onoga što si" odnosi se na ponašanje i fizičke atribute, "Na temelju onoga što posjeduješ" se odnosi na dokument ili akreditiv i "na temelju onoga što znaš" se odnosi na lozinke, osobne informacije, itd.

"Fizički atributi"
Ljudi često identificiraju druge ljude koje znaju po njihovom izgledu. Specifične značajke za tu svrhu su spol, visina, težina, rasa, boja očiju i kose, itd. Atributi koji su jedinstveni za svaku individualnu osobu su često najkorisniji, to uključuje otisak prsta ili skenirana rožnica. Ponekad su automatske identifikacijske sheme bazirane na biometriji poput dviju prethodno navedenih. Pretpostavlja se da će se biometrija koristiti još češće u budućnosti.

"Akreditiv"
U diplomatskom korištenju riječi akreditiv je uvodno slovo. Sigurni dokumenti ili kartice kao na primjer vozačka dozvola ili putovnica funkcioniraju kao akreditiv u mnogim situacijama. Napomenimo da akreditiv često uključuje fotografije koje pomažu fizičkoj identifikaciji nosioca akreditiva.

"Znanje"
Znanje je često korišteno za identifikaciju kada se osoba koja se treba identificirati ne nalazi na istoj lokaciji kao i osoba koja vrši identifikaciju. U kontekstu identifikacije, znanje može biti password ili PIN (personal identification number), ili majčino djevojačko prezime. Poteškoća kod korištenja znanja kao identifikacije je ta da znanje ne mora biti tajna, i često je otkrivena kao dio identifikacijskog procesa. To omogućuje lažno predstavljanje osobe koja se identificira, što nije dobro. Kako god, prikladni kriptografski protokoli će dozvoliti konstrukciju sigurne identifikacijske sheme koja će spriječiti lažno predstavljanje.

Neke od svakodnevnih situacija u kojima se dokazuje nečiji identitet, osobno ili elektronski su sljedeće:

"Telefonske kartice"
Da bi naplatili telefonski poziv korištenjem telefonske kartice potrebno je samo znanje telefonskog broja koji se naplaćuje za poziv, zajedno sa četveroznamenkastim PIN-om.

"Prijava na daljinu" (remote login)
Da bi se spojili na udaljeno računalo preko interneta s telnet ili ssh opcijom potrebno je znati korisničko ime i njegovu loziku.

"Kupovina kreditnim karticama unutar trgovine"
Kada se kreditnom karticom kupuje u trgovini, prodavač treba potvrditi da je potpis kupca identičan potpisu s stražnje strane kartice. To je primjer slabe identifikacijske forme zato što je potpis moguće lako krivotvoriti. Neke kreditne kartice imaju i sliku vlasnika koja je dodatni nivo autentikacije. Drugi način za poboljšanje zaštite korisnika je kroz PIN (personal identification number) koji je korišten za kartice koje imaju čip.

"Kupovina kreditnom karticom bez prisustva kreditne kartice"
U mnogim situacijama prisustvo kreditne kartice nije potrebno da bi se ona koristila. Na primjer, da bi kupili proizvod putem interneta kreditnom karticom sve što je potrebno je broj kreditne kartice i datum njezina isteka. Takvo korištenje kreditne kartice ne pruža dovoljnu sigurnost zato što ne postoji prava autentikacija identiteta. Baš zato bilo tko može kupovati vašom karticom preko interneta ako posjeduje broj vaše kreditne kartice i datum isteka.

"Podizanje novca na bankomatu"
Da bismo podigli novac na bankomatu koristimo bankovnu karticu zajedno s četvero ili šesteroznamenkastim PIN-om. Kadtica sadrži ime vlasnika i informacije o njegovom bankovnom računu. Svrha PIN-a je zaštita korištenja kartice od strane pogrešne osobe. Pretpostavka je da je jedina osoba koja zna PIN vlasnik kartice.

U praksi, većina od gore navedenih tipova nije implementirana na siguran način. U protokolima izvršenim putem telefona, bilo koji prisluškivač razgovora može koristiti identifikacijske informacije za svoje potrebe. Čak i osobe koje traže informacije korisnika putem telefona se znaju predstavljati lažno da bi dobile informacije o kreditnim karticama od korisnika. Bankovne kartice su malo sigurnije, ali imaju svoje slabosti. Na primjer, osobe koje prate komunikacijsku liniju mogu se dočepati informacija šifriranih na magnetnoj traci kartice kao i njezinog PIN-a. To bi moglo omogućiti varalicama pristup tuđem bankovnom računu. Spajanje računalom na daljinu je ozbiljan problem ako su ID-jevi i šifre poslani

putem mreže u nekriptiranoj formi zato što mogu biti pročitani od strane bilo koga tko je spojen na računalnu mrežu.

Cilj identifikacijske sheme bi bio da se onaj tko prisluškuje Anu, ne može kasnije lažno predstavljati kao ona. Model napada dopušta protivniku promotriti sve informacije koje su prenesene između Ane i Borisa. Možemo se pokušati zaštititi od mogućnosti da će sam Boris pokušati oponašati Anu nakon što zna da je to ona. Konačno, željeli bismo osmisliti shemu "bez znanja" gdje Ana svoj identitet može potvrditi elektroničkim putem, bez "odavanja" informacija koje se koriste kao njezine informacije za identifikaciju.

Nekoliko praktičnih i sigurnih identifikacijskih shema su otkrivene. Jedan cilj je pronaći shemu koja je dovoljno jednostavna da bi se mogla implementirati na pametne kartice. U većini slučajeva to se odnosi na kreditne kartice koje sadrže čip koji obavlja aritmetička računanja. Količina računanja i potrebna memorija trebaju biti što je moguće manje. Takva kartica bila bi sigurnija od većine trenutnih kreditnih kartica. Važno je napomenuti da se "dodatna" sigurnost odnosi na nekoga ko nadgleda komunikacijsku liniju. Pošto je kartica ta koja "dokazuje" vlasnikov identitet, nemamo "dodatnu" sigurnost za izgubljene kartice. I dalje bi bilo potrebno uključiti PIN da bi se ustanovilo da li je pravi vlasnik kartice pokrenuo indentifikacijsku shemu.

Prvo zapažanje je da bilo koja identifikacijska shema treba uključivati randomizaciju na neki način. Kad bi informacija koju Ana prenosi Borisu da se identificira uvijek ostajala nepromijenjena tada je shema nesigurna po modelu koji je spomenut iznad.

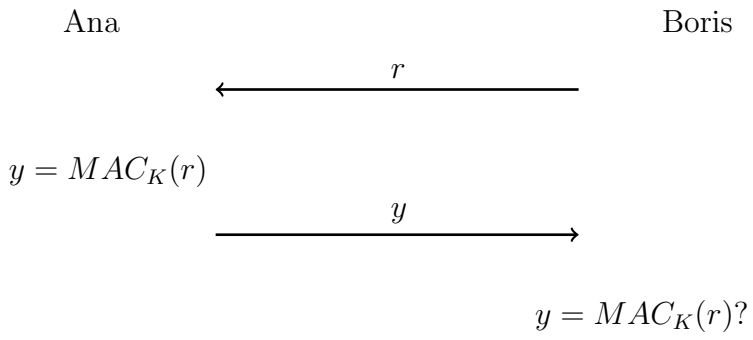
Algoritam 1 (Nesigurni Izazov-i-odgovor)

1: Boris odabere nasumičan izazov "r" koji pošalje Ani.
2: Ana izračuna $y = MAC_K(r)$ i pošalje y nazad Borisu.
3: Boris izračuna $y' = MAC_K(r)$ i ako je $y' = y$ prihvaća, u suprotnom odbija.

Zato sigurnosne identifikacijske sheme obično sadrže "nasumičan izazov" u sebi. Ovaj koncept je bolje objašnjen u sledećem poglavlju. Uzeti ćemo dva pristupa za dizajniranje identifikacijske sheme. Prvi, u kojem ćemo istražiti ideju izgradnje sigurne identifikacijske sheme iz jednostavnijih kriptografskih primitivaca, to jest, kod za ovjeru poruke ili potpisna shema. Ove sheme su analizirane u poglavljima 2 i 3, a u ostalim dijelovima rada raspravljamo o tri identifikacijske sheme koje su izgrađene "od nule". Te sheme su nazvane po Schnorru, Okamotou i Guillou-Quisquateru.

2 Izazov-i-odgovor i postavke tajnoga ključa

U daljim poglavljima, opisat ćemo neke od popularnijih identifikacijskih shema za koje nije potrebno prethodno znanje. Prvo pogledajmo identifikaciju u postavkama tajnoga ključa, gdje Ana i Boris posjeduju isti tajni ključ. Počinjemo s promatranjem vrlo jednostavne (ali nesigurne) sheme koja je bazirana na bilo kojem kodu za ovjeru poruke. Shema prikazana u Algoritmu 1 zove se Izazov-i-odgovor. U njoj pretpostavljamo da se Ana identificira Borisu i njihov zajednički tajni ključ je označen s K (Boris se isto može identificirati Ani, samo zamjenimo uloge Ane i Borisa u shemi). Kod za autentikaciju poruka (message authentication code) MAC_K koristi se za izračunavanje autentikacijskih tagova (oznaka za provjeru autentičnosti). Često ćemo interaktivne protokole prikazivati u obliku dijagrama. Algoritam 1 bi se mogao prikazati kao Slika 2.1.



Slika 2.1: Tok informacija u Algoritmu 1.

Prije analize slabosti ove sheme, definirajmo osnovnu terminologiju povezanu s interaktivnim protokolima. Općenito, interaktivni protokol će uključivati dvije ili više stranaka koje komuniciraju međusobno.
Svaka stranka je modelirana algoritmom koji naizmjenično šalje i prima informacije. Svako pokretanje protokola zovemo sesijom. Svaki korak unutar sesije protokola naziva se tok. Tok se sastoji od informacija poslanih od strane jedne stranke drugoj (Algoritam 1 sastoji se od dva toka, prvi od Borisa do Ane i drugi od Ane do Borisa). Na kraju sesije, Boris (pokretač sesije) "prihvaća" ili "odbija". Ana ne mora znati da li je Boris prihvatio ili nije. Nije teško primjetiti da je Algoritam 1 nesiguran, čak i ako smo korisitili kod za autentikaciju poruke koji je siguran. Osjetljiv je na prilično standardnu vrstu napada poznatu pod nazivom Paralelni napad na sesiju gdje se Marko predstavlja kao Ana (oponaša Anu). Unutar prve sesije (u kojoj pretpostavimo da se Marko predstavlja, kao Ana, Borisu) Marko pokrene drugu

sesiju u kojoj pita Borisa da se identificira. U drugoj sesiji Marko da Borisu isti izazov koji je primio od Borisa u prvoj sesiji. Kada dobije Borisov odgovor, Marko nastavlja prvu sesiju u kojoj pošalje Borisov odgovor nazad Borisu. Na taj način Marko uspješno izvrši prvu sesiju.

Algoritam 2 ((Siguran) Izazov-i-odgovor)

1: Boris odabire nasumičan izazov, r, koji pošalje Ani.
2: Ana izračuna $y = MAC_K(ID(Ana)||^1 r)$ i pošalje y Borisu.
3: Boris izračuna $y' = MAC_K(ID(Ana)||r)$ i ako je $y' = y$ prihvaća, u suprotnom odbija.

Postoje scenariji u kojima paralelne sesije mogu biti razumne ili čak poželjne, i čini se pametno dizajnirati identifikacijsku shemu koja će moći izdržati takve napade. Predstavljamo jedan lagani način za popravljanje problema u Algoritmu 2. Jedina promjena koja se treba napraviti je ta da treba uključiti identitet osobe koja kreira MAC unutar izračuna autentikacijskog taga (Oznake za provjeru autentičnosti).
Pretpostavit ćemo da je u Algoritmu 2 nasumičan izazov bitstring specificirane, već predodređene duljine, recimo k bitova (u praksi, $k = 100$ bi bio pogodan izbor). Također, pretpostavimo da je identifikacijski string ($ID(Ana)$ ili $ID(Boris)$, u ovisnosti čiji identitet se autenticira) isto bitstring određene duljine, formatiran nekim standardnim, fiksnim načinom. Pretpostavimo da identifikacijski string sadrži dovoljno informacija da odredi jedinstvenog pojedinca unutar mreže (dakle Boris se ne treba brinuti s kojom "Anom" priča).
Tvrdimo da se paralaleni sesijski napad ne može izvršiti protiv Algoritma 2.
Ako Marko pokuša izvesti isti napad kao prije, dobio bi vrijednost $MAC_K(ID(Boris)||r)$ od Borisa u drugoj sesiji. To mu ne bi pomoglo pri izračunu $MAC_K(ID(Ana)||r)$ koji je potreban u prvoj sesiji da bi uspješno odgovorio Borisovom izazovu. Prethodna rasprava bi nas mogla uvjeriti da paralelni sesijski napad ne može biti iskorišten protiv Algoritma 2, ali to nam ne dokazuje da je algoritam siguran od svih mogućih napada. Uskoro ćemo dati dokaz sigurnosti. Prvo ćemo navesti sve pretpostavke koje imamo:

1. **Tajni ključ**
   Pretpostavimo da je tajni ključ, K, poznat samo Ani i Borisu.

2. **Nasumični izazovi**
   Pretpostavimo da Ana i Boris imaju savršen generator nasumičnih brojeva koji koriste da odrede njihove izazove. Zbog toga postoji jako mala vjerojatnost da se isti izazov ponovi u dvije različite sesije.

[1] || označava konkatanaciju stringova

3. **MAC sigurnost**
   Pretpostavimo da je kod za autentikaciju poruke siguran. Preciznije, da ne postoji (ϵ, Q)-falsifikator za MAC, za odgovarajuće vrijednosti ϵ i Q. Vjerojatnost da Marko može točno izračunati $MAC_K(x)$ je najviše ϵ, čak i kada mu je dan Q drugih MAC-ova, recimo $MAC_K(x_i)$, $i = 1, 2, \ldots, Q$, gdje je $x \neq x_i$ za svaki i. Q je specificiran (određen) sigurnosni parametar ($Q = 10000$ ili 100000 može biti razuman odabir, ovisno o aplikaciji).

Marko može promatrati nekoliko sesija između Ane i Borisa. Markov cilj je prevariti Anu ili Borisa, tj. učiniti da Boris "prihvati" sesiju u kojoj Ana nije sudjelovala ili da Ana "prihvati" sesiju u kojoj Boris ne sudjeluje. Pokazat ćemo da Marko neće uspjeti prevariti Anu i Borisa na ovaj način, kada su važeće iznad navedene pretpostavke, osim s malom vjerojatnošću. To ćemo napraviti vrlo jednostavno, samom analizom strukture sheme.
Pretpostavimo da Boris "prihvaća". Tada je $y = MAC_K(ID(Ana)||r)$, gdje je y vrijednost koju prima u drugom toku, a r je njegov izazov iz prvog toka sheme. S velikom vjerojatnošću tvrdimo da je vrijednost y konstruirana od strane Ane kao odgovor na izazov r iz prvog toka sheme. Da opravdamo tvrdnju, pretpostavimo moguće izvore odgovora ako on nije došao direktno od Ane. Prvo, zato što je za ključ K predpostavljeno da ga znaju samo Ana i Boris, ne moramo razmišljati o vjerojatnosti da je $y = MAC_K(ID(Ana)||r)$ izračunato od strane nekoga drugog ko zna ključ K. Dakle Marko je izračunao y bez poznavanja ključa K, ili je vrijednost y, koja je bila izračunata od strane Ane ili Borisa u nekoj od prethodnih sesija, kopirana i iskorištena od Marka u trenutnoj sesiji. Pretpostavimo moguće slučajeve redom:

1. Pretpostavimo da je vrijednost $y = MAC_K(ID(Ana)||r)$ prethodno konstruirana od strane Borisa u nekoj od prethodnih sesija. Znamo da Boris samo izračunava MAC-ove od forme $MAC_K(ID(Boris)||r)$ dakle on nije sam kreirao y. Stoga se ovaj slučaj neće dogoditi.

2. Pretpostavimo da je y prethodno konstruirana od strane Ane u nekoj od prethodnih sesija. To se moglo dogoditi samo ako je izazov r ponovljen. Za r smo pretpostavili da je novokreiran izazov od strane Borisa korištenjem savršenog generatora nasumičnih brojeva, pa stoga Boris ne bi trebao imati isti izazov u nekoj drugoj sesiji, osim s malom vjerojatnošću da se broj ipak ponovio.

3. Pretpostavimo da je y novi MAC koji je konstruiran od strane Marka. Pošto smo pretpostavili da je kod za autenticiranje poruke (MAC) siguran i da Marko ne zna ključ K, Marko ne može to napraviti, osim s jako malom vjerojatnošću.

Neformalan dokaz dan iznad može biti precizniji. Kad bi mogli dokazati ekplicitno, preciznu izjavu o sigurnosti ishodišnog MAC-a, onda bi mogli dati precizno sigurnosno jamstvo

za identifikacijsku shemu. To je moguće ako je MAC bezuvjetno siguran. Alternativno, ako damo pretpostavku o sigurnosti MAC-a, onda možemo predvidjeti sigurnosni rezultat za identifikacijsku shemu koja ovisi o toj pretpostavci (ovo je uobičajeni model za dokaz sigurnosti). Vjerojatnost da će osoba prevariti Borisa ako je ona aktivni sudionik sheme, proporcionalno ovisi o sigurnosnom mehanizmu identifikacijske sheme. Za MAC kažemo da je bezuvjetno (ϵ, Q)-siguran ako prevarant ne može konsturirati važeći MAC za bilo koju novu poruku s vjerojatnošću većom od ϵ, ako znamo da je prevarant prije toga vidio važeći MAC za Q poruka (ne postoji (ϵ, Q)-falsifikator). Pretpostavimo da je fiksni ključ K, čiju vrijednost prevarant ne zna, korišten za konstruiranje svih Q-ova MAC-a. Identifikacijska shema je definirana kao bezuvjetno (ϵ, Q)-sigurna ako prevarant ne može prevariti Anu i Borisa da prihvate s vjerojatnošću većom od ϵ, iako je prevarant promatrao najviše Q prethodnih sesija između Ane i Borisa.
Bezuvjetno (ϵ, Q)-sigurni MAC-ovi postoje za bilo koju vrijednost Q i ϵ. Međutim, bezuvjetno sigurni MAC-ovi obično zahtjevaju velike ključeve (posebice ako je Q velik). Kao posljedica, računalno sigurni MAC-ovi kao na primjer CBC-MAC su češće korišteni u praksi. U ovoj situaciji je potrebna pretpostavka o sigurnosti MAC-a. Ova bi pretpostavka imala sličan oblik, ali može uključivati vrijeme kao eksplicitni parametar. Za MAC kažemo da je (ϵ, Q, T)-siguran ako prevarant ne može konstruirati važeći MAC za bilo koju novu poruku s vjerojatnošću većom od ϵ, gdje je vrijeme računanja najviše T i da je prije toga vidio važeći MAC za najviše Q poruka. Identifikacijska shema je definirana kao (ϵ, Q, T)-sigurna ako prevarant ne može prevariti Anu i Borisa da prihvate s vjerojatnošću većom od ϵ, znajući da je prevarant promatrao najviše Q prethodnih sesija između Ane i Borisa, i da je prevarantovo vrijeme računanja najviše T.

Zbog jednostavnijeg obilježavanja ćemo izostavljati ekplicitnu specifikaciju vremenskog parametra. To će nam omogućiti korištenje sličnih notacija u računalno sigurnim i bezuvjetno sigurnim postavkama. Bit će jasno iz konteksta pričamo li o bezuvjetnoj ili računalnoj sigurnosti. Pretpostavimo prvo da baziramo identifikacijsku shemu na bezuvjetno sigurnom MAC-u. Tada će rezultat identifikacijske sheme biti također bezuvjetno siguran, znajući da prevarant ima pristup najviše Q važećih MAC-ova kroz nekoliko kolekcija sesija gdje sve koriste isti MAC ključ. Trebamo se prisjetiti jednog dodatnog parametra - veličine (u bitovima) slučajnog izazova korištene u shemi, koja je označena sa k. Pod tim uvjetima, možemo lako dati gornju granicu vjerojatnosti da će prevarant prevariti Borisa. Promotrimo ista tri slučaja kao i prije:

1. Kao što smo već utvrdili, vrijednost $y = MAC_K(ID(Ana)||r)$ nije prethodno konstruirana od strane Borisa u nekim od drugih sesija (pa se ovaj slučaj neće dogoditi).

2. Pretpostavimo da je vrijednost y prethodno konstruirana od strane Ane u nekoj od drugih sesija. Za izazov r pretpostavimo da je slučajan izazov novokreiran od strane Borisa. Vjerojatnost da je Boris već koristio izazov r u nekoj od prethodnih sesija je $\frac{1}{2^k}$. Postoji najviše Q prethodnih sesija za razmotriti, dakle vjerojatnost da je r korišten kao izazov u jednoj od tih prethodnih sesija je najviše $\frac{Q}{2^k}$. Ako se to dogodi, tada prevarant može ponovno upotrijebiti MAC iz prethodne sesije (Točna vjerojatnost da je izazov iz prethodne sesije ponovljen je $1-(1-2-k)^Q$ što je manje od $\frac{Q}{2^k}$).

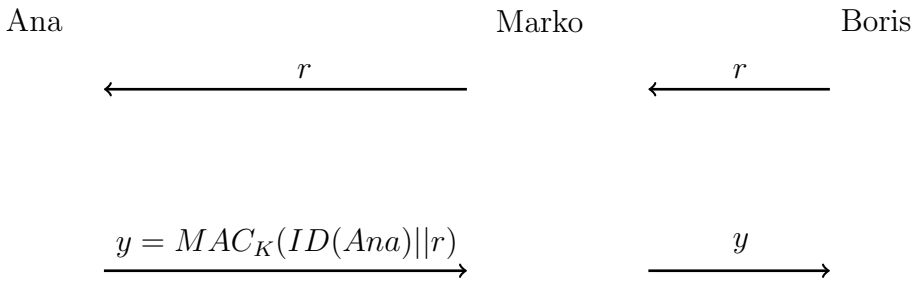
3. Pretpostavimo da je vrijednost y novi MAC koji je konstruiran od strane Marka. Marko će biti uspješan u prevari s vjerojatnošću najviše ϵ; To dobijemo iz sigurnosti MAC-a koji je korišten.

U konačnici, vjerojatnost da Marko prevari Borisa je najviše $\frac{Q}{2^k}+\epsilon$. Stoga smo uspostavili sigurnost identifikacijske sheme kao funkciju sigurnosti temeljnih primitiva. Analiza je identična ako koristimo računalno siguran MAC. Sumirat ćemo rezultat iz ovog poglavlja sljedećim teoremom.

Teorem 2.1. *Pretpostavimo da je MAC (ϵ, Q)-siguran MAC, i pretpostavimo da su nasumični izazovi dugački k bitova. Tada je Algoritam 2 $(\frac{Q}{2^k}+\epsilon, Q)$-sigurna identifikacijska shema.*

3 Model napada i protivnički ciljevi

Postoji nekoliko vještina povezanih s modelom napada i protivničkim ciljevima u identifikacijskoj shemi. Kao demonstraciju opisat ćemo "uljez-u-sredini" scenarij na Slici 3.1. Na prvi pogled, ovo može izgledati kao paralelni sesijski napad. Moglo bi se tvrditi da Marko oponaša Anu Borisu u jednoj sesiji, i da oponaša Borisa Ani u paralelnoj sesiji. Kad Marko primi Borisov izazov r, pošalje ga Ani. Tada odgovor od Ane (y) Marko pošalje Borisu, i Boris će prihvatiti. Svejedno, ovakav napad ne smatramo pravim napadom, zato što je "unija" dvije sesije zapravo jedna sesija u kojoj se Ana uspješno identificirala Borisu. Konačan rezultat je da je Ana izračunala i dala točan odgovor y na Borisov izazov.



Slika 3.1: Uljez u sredini

Marko jednostavno proslijedi poruke određenoj osobi bez da ih modificira, pa Marko nije aktivni učesnik sheme. Sesija se izvršila točno kako i bi bez da je Marko bio učesnik.
Jasna formulacija protivničkog cilja trebala bi nam omogućiti da pokažemo da ovo nije napad. Pristupit ćemo dokazu na sljedeći način. Kažemo da je Marko aktivan učesnik sesije ako vrijedi nešto od sljedećeg:

1. Marko kreira novu poruku i stavlja ju u kanal.
2. Marko mijenja poruku u kanalu.
3. Marko preusmjerava poruku u kanalu tako da je šalje nekome tko nije osoba inače namijenjena primanju poruke.

Cilj prevaranta je da pokretač sheme (u ovom slučaju Boris, za kojeg pretpostavljamo da je iskren) "prihvati" u nekoj od sesija u kojoj je prevarant aktivan sudionik. Prema ovoj definiciji, Marko nije aktivan u gore razmatranom "uljez-u-sredini" scenariju, i zato

protivnički cilj nije realiziran. Drugi, bitno ekvivalentan, način za odluku je li prevarant stvarno aktivan je razmotriti Anin i Borisov pogled na shemu. I Ana i Boris su unaprijed određeni sudionici u komunikaciji: Ana je određena Borisu, i Boris je određen Ani. Nadelje, ako ne postoji aktivni prevarant, tada bi Ana i Boris imali odgovarajući prikaz sesije: svaka poruka poslana od Ane je primljena od strane Borisa i obrnuto. Također, sve poruke će biti primljene u točnom redoslijedu. Ove karakteristike sesije su ponekad opisane kao "podudaranje razgovora".

Gore navedena rasprava o modelu pretpostavlja da su legitimni sudionici sesije iskreni. Da budemo precizniji, sudionik unutar sesije sheme je iskren sudionik ako on/ona slijedi shemu, obavlja točno računanje, i ne otkriva informacije prevarantu. Ako sudionik nije iskren, tada je shema kompletno porušena, pa zato iskazi o sigurnosti obično zahtjevaju da sudionici budu iskreni.

Razmotrimo sada model napada. Prije nego zapravo pokuša prevariti Borisa, Marko se bavi fazom prikupljanja podataka. Marko je pasivni prevarant tijekom te faze ako samo promatra sesiju između Borisa i Ane. Alternativno, možemo uzeti u obzir i model napada u kojem je Marko aktivan tijekom faze prikupljanja podataka. Na primjer, Marko može dobiti privremeni pristup predviđanju koje izračunava autentikacijske oznake $MAC_K(\cdot)$ za nepoznati ključ K kojeg koriste Ana i Boris. Tijekom tog razdoblja, Marko može uspješno prevariti Anu i Borisa, koristeći predviđanje da koje će odgovarati na izazove. Nakon faze prikupljanja podataka, MAC predviđanje je otuđeno, i tada Marko provodi svoj napad, pokušavajući nasamariti Anu i Borisa da "prihvate" u novoj sesiji u kojoj Marko nema MAC predviđanje. Analiza sigurnosti koja je obavljenja u Poglavlju 2 odnosi se na oba gore navedena modela napada. Identifikacijska shema je dokazivo sigurna (točnije, vjerojatnost da prevarant uspije je najviše $\frac{Q}{2^k} + \epsilon$) u pasivnom modelu prikupljanja podataka pod uvjetom da je MAC (ϵ, Q)-siguran protiv napada poznatim tekstom. Nadalje, identifikacijska shema je sigurna u aktivnom modelu prikupljanja podataka pod uvjetom da je MAC (ϵ, Q)-siguran protiv izabranog tekstualnog napada.

3.1 Međusobna provjera autentičnosti

Shema u kojoj Ana i Boris dokazuju svoj identitet jedno drugome naziva se **Međusobna provjera autentičnosti** ili **Međusobna provjera identifikacije**. Oba sudionika su potrebna "prihvatiti" ako se sesija sheme smatra uspješnom sesijom. Prevarant može pokušati prevariti ili Anu ili Borisa ili oboje da prihvate. Protivnički cilj je prouzrokovati iskrenog učesnika da "prihvati" nakon toka u kojem je prevarant bio aktivan. Sljedeći uvjeti određuju koji je ishod sheme međusobne provjere identifikacije, ako je shema smatrana sigurnom:

1. Pretpostavimo da su Ana i Boris dva sudionika u sesiji sheme i oboje su iskreni. Pretpostavimo također da je prevarant pasivan. Tada i Ana i Boris "prihvaćaju".

2. Ako je prevarant aktivan tijekom danog toka sheme, tada niti jedan iskreni sudionik neće "prihvatiti".

Primjetimo da prevarant može biti neaktivan u određenoj sesiji dok jedan sudionik ne prihvati, a onda može postati aktivan. Zato je moguće da jedan iskren sudionik "prihvati" pa onda drugi iskren sudionik "odbije". Prevarant ne postiže cilj u ovom scenariju, iako sesija nije u potpunosti dovršena, zato što je prevarant bio inaktivan prije nego što je prvi sudionik prihvatio. Ishod sesije je da će se Ana uspješno identificirati Borisu, ali Boris se neće uspješno identificirati Ani.

Algoritam 3 (Nesiguran međusobni izazov-i-odgovor)

1: Boris odabere nasumičan izazov, r_1, koji pošalje Ani.
2: Ana odabere nasumičan izazov, r_2 i izračuna $y_1 = MAC_K(ID(Ana)||r_1)$ i pošalje r_2 i y_1 Boris.
3: Boris izračuna: $y_1' = MAC_K(ID(Ana)||r_1)$. Ako je $y_1' = y_1$, tada Boris "prihvaća"; u suprotnom Boris "odbija". Boris također izračuna $y_2 = MAC_K(ID(Boris)||r_2)$ i pošalje y_2 Ani.
4: Ana izračuna $y_2' = MAC_K(ID(Boris)||r_2)$. Ako je $y_2' = y_2$, tada Ana "prihvaća"; u suprotnom Ana "odbija".

Ovo možemo smatrati prekidom sheme, ali to nije uspješan napad. Postoji nekoliko načina u kojima prevarant može biti aktivan u sesiji sheme. Navest ćemo neke od njih:

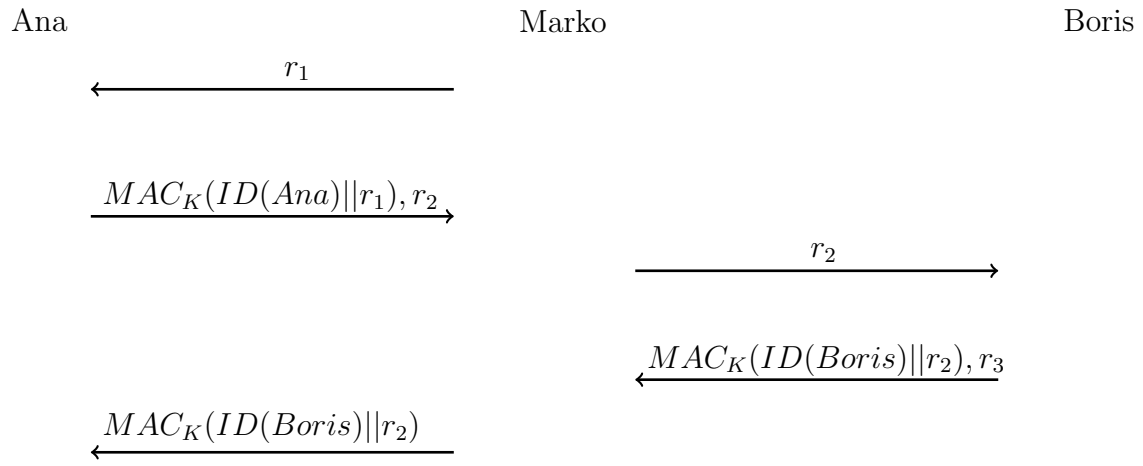
1. Prevarant oponaša Anu, nadajući se da će Boris prihvatiti.

2. Prevarant oponaša Borisa, nadajući se da će Ana prihvatiti.

3. Prevarant je aktivan u nekim sesijama u kojima su Ana i Boris upleteni, i on pokušava obmanuti Anu i Borisa da prihvate.

Možemo pokušati ostvariti međusobnu provjeru autentičnosti pokretanjem Algoritma 2 dva puta (npr. Ana potvrdi Borisov identitet, i Boris potvrdi Anin identitet u odvojenim sesijama). Ali generalno je učinkovitije dizajnirati jednu shemu za postizanje obje identifikacije odjednom. Što ako bi Ana i Boris spojili dvije sesije jednosmjerne identifikacije u jednu shemu, na očigledan način? Upravo to je napravljeno u Algoritmu 3, i smanjen je broj potrebnih tokova sa četiri na tri (u usporedbi s dvostrukim korištenjem originalne jednosmjerne sheme). Rezultirajuća shema međusobne provjere identičnosti je svejedno nesavršena i može biti napadnuta. Algoritam 3 je nesiguran zato što Marko može obmanuti Anu s paralelnim

sesijskim napadom. Marko, pretvarajući se da je Boris, pokrene sesiju s Anom. Kada Marko primi Anin izazov, r_2, u drugom toku, on "prihvati, i pokrene novu sesiju s Borisom (u kojoj se pretvara da je Ana).



Slika 3.2: Napad na Algoritam 3.

U drugoj sesiji, Marko pošalje r_2 Borisu kao njegov izazov u prvom toku. Kada Marko dobije Borisov odgovor (u drugom toku druge sesije), prosljedi ga Ani kao treći tok prve sesije. Ana će "prihvatiti", i tako će Marko uspješno oponašati Borisa u sesiji. (Druga sesija je odbačena, i neće biti završena.) Ovo sačinjava uspješan napad, zato što je iskreni sudionik u prvoj sesiji (Ana) prihvatio nakon toka (inicijalni tok sesije) u kojem je Marko bio aktivan. Na Slici 3.2 možemo vidjeti prikaz tog napada.

Kao što možemo primjetiti, napad je baziran na ponovnom korištenju toka iz jedne sesije u drugom toku različite sesije. Problem nije teško popraviti, zapravo postoji nekoliko načina na koje je moguće modificirati shemu da bude sigurna. U osnovi, potrebno je dizajnirati tok tako da svaki tok sadrži informacije koje se izračunavaju na različit način. Jedno rješenje je prikazano u Algoritmu 4.

Jedina promjena koja je napravljena u Algoritmu 4 je u definiciji y_1 u koraku 2. Sada ovaj MAC ovisi o dva izazova, r_1 i r_2. To nam je potrebno da bi razlikovali drugi tok od trećeg toka (u kojem MAC ovisi samo o izazovu r_2).

Algoritam 4 ((Siguran) Međusobni izazov-i-odgovor)

1: Boris odabere nasumičan izazov, r_1, koji pošalje Ani.
2: Ana odabare nasumičan izazov, r_2 i izračuna $y_1 = MAC_K(ID(Ana)||r_1||r_2)$ te pošalje r_2 i y_1 Borisu.
3: Boris izračuna $y_1' = MAC_K(ID(Ana)||r_1||r_2)$. Ako je $y_1' = y_1$, tada Boris "prihvaća", a u suprotnom "odbija". Boris također izračuna: $y_2 = MAC_K(ID(Boris)||r_2)$ i pošalje y_2 Ani.
4: Ana izračuna $y_2' = MAC_K(ID(Boris)||r_2)$. Ako je $y_2' = y_2$ tada Ana "prihvaća", a u suprotnom "odbija".

Algoritam 4 može biti analiziran na sličan način kao Algoritam 2, malo kompliciranije, zato što se prevarant može predstavljati kao Boris (želi prevariti Anu) ili kao Ana (želi prevariti Borisa). Vjerojatnost da se vrijednosti y_1 ili y_2 mogu "ponovno iskoristiti" iz prethodnih sesija može biti izračunata, kao i vjerojatnost da prevarant može izračunati novi MAC od početka (od nule/od ničega postojećeg).

Zato što se svaka vrijednost y_1 izračunava na različit način od vrijednosti y_2, nemoguće je da y_1 vijednost iz jedne sesije može biti ponovno iskorištena kao y_2 vrijednost u drugoj sesiji (ili obrnuto). Marko može pokušati imitirati Borisa (prevariti Anu) ili Ana (prevariti Borisa), određivanjem y_1 ili y_2. Vjerojatnost da se y_1 ili y_2 mogu ponovno iskoristiti iz prethodnih sesija je najviše $\frac{Q}{2^k}$, pod pretpostavkom da je Marko vidio najviše Q MAC-ova iz prethodnih sesija (ovo ograničava broj prethodnih sesija na $\frac{Q}{2}$, zato što su tu dva MAC-a po sesiji). Vjerojatnost da Marko može izračunati novi y_1 je najviše ϵ, i vjerojatnost da može izračunati novi y_2 je također najviše ϵ. Zato je vjerojatnost da Marko može prevariti Anu ili Borisa jednaka najviše $\frac{Q}{2^k} + 2\epsilon$. Sumiranjem svega dobivamo sljedeći teorem.

Teorem 3.1. *Pretpostavimo da je MAC (ϵ, Q)-siguran kod za ovjeru poruke, i pretpostavimo da su nasumični izazovi dugački k bitova. Tada je Algoritam 4 $(\frac{Q}{2^k} + 2\epsilon, \frac{Q}{2})$-sigurna međusobna identifikacijska shema.*

4 Izazov-i-odgovor u postavkama javnog ključa

Sada se okrećemo postavci javnog ključa, gdje Ana i Boris možda nemaju zajednički tajni ključ. Pretpostavimo da su Ana i Boris članovi mreže, u kojoj svaki sudionik ima javni i privatni ključ za unaprijed određeni kriptosustav i/ili potpisni plan. U postavci kao što je ova, uvijek je potrebno pružiti mehanizam za autentikaciju javnog ključa drugih ljudi iz mreže. Ovo zahtjeva neku vrstu infrastukture javnog ključa (označeno sa PKI (public-key infrastucture)). Pretpostavimo da postoji sustav nadležnosti, označen s TA, koji obilježava javne ključeve za sve sudionike mreže. Pretpostavimo da je javna verifikacija ključa od TA, označena s ver_{TA}, znana svim ljudima u mreži. Ova pojednostavljena postavka nije u potpunosti realna, ali pomoći će nam da se koncentriramo na dizajn sheme.

4.1 Certifikati

Certifikat za korisnika mreže će sadržavati neku identifikacijsku informaciju za tu osobu (na primjer njihovo ime, email adresu...), njen javni ključ/javne ključeve, i potpis od TA na toj informaciji. Certifikat dopušta korisniku mreže da potvrdi autentičnost svih drugih ključeva. Pretpostavimo, za primjer, da Ana želi dobiti certifikat od TA koji sadrži kopiju Aninog javnog verifikacijskog ključa za potpisni plan. Tada će se odraditi koraci kao u Algoritmu 5.

Algoritam 5 (Izdavanje certifikata Ani)

1: TA utvrđuje Anin identitet pomoću uobičajenog oblika identifikacije kao što su rodni list, putovnica.... Tada TA formira string, oznake $ID(Ana)$, koji sadrži Aninu identifikacijsku informaciju.
2: Privatni potpisni ključ za Anu, sig_{Ana}, i odgovarajući javni verifikacijski ključ, ver_{Ana}, su određeni.
3: TA generira svoj potpis $s = sig_{TA}(ID(Ana)||ver_{Ana})$ na Aninom indentifikacijskom stringu i verifikacijskom ključu. Certifikat $Cert(Ana) = (ID(Ana)||ver_{Ana}||s)$ je dan Ani, zajedno s Aninim privatnim ključem, sig_{Ana}.

Nećemo točno specificirati kako se Ana identificirala TA, niti ćemo precizirati format od $ID(Ana)$, ili kako su javni i privatni ključevi od Ane odabrani. Općenito, ti implementacijski detalji mogu varirati od jedne infrastrukture javnog ključa do druge. Moguće je za bilo koga tko zna TA verifikacijski ključ, ver_{TA}, da potvrdi bilo čiji certifikat. Pretpostavimo da Boris želi biti siguran da je Anin javni ključ autentičan. Ana može dati svoj certifikat Borisu. Boris tada može potvrditi potpis od TA tako da provjeri: $ver_{TA}(ID(Ana)||ver_{Ana}, s) = true$. Sigurnost certifikata slijedi iz sigurnosti potpisnog plana korištenog od strane TA.

Kao što je ranije spomenuto, smisao verificiranja certifikata je da se autenticira nečiji javni ključ. Certifikat sam po sebi ne pruža nikakvu vrstu dokaza identiteta, zato što certifikati sadrže samo javne informacije. Certifikati mogu biti proizvedeni ili ponovno napravljeni za bilo koga, i posjed certifikata ne implicira njegovo vlasništvo.

4.2 Identifikacijske sheme javnoga ključa

Sada pogledajmo međusobnu identifikacijsku shemu u postavkama javnoga ključa. Naš plan je modificirati Algoritam 4 tako da zamjenimo MAC-ove sa potpisom. Druga razlika je ta, da u postavci tajnog ključa, uključujemo ime osobe koja je napravila MAC u svakom MAC-u (to je bilo potrebno zato što tajni ključ K, znan dvjema grupama, dopušta bilo kojoj grupi da kreira MAC-ove). U postavkama javnog ključa, samo jedna osoba može kreirati potpise koristeći specifični privatni potpisni ključ, drugim riječima, samo osoba koja posjeduje taj ključ. Zbog toga mi ne moramo eksplicitno imenovati tko je kreirao određeni potpis. Dok u postavci tajnog ključa, na početku sesije, svaki sudionik ima osobu s kojom želi komunicirat. Svaki sudionik će koristiti verifikacijski ključ željene osobe da verificira potpis primljen u predstojećoj sesiji i također uključiti ime željene osobe u svim potpisima koje kreira tijekom sheme.

Algoritam 6 (Međusobna autentikacija javnoga ključa (prva verzija))

1: Boris odabere nasumičan izazov, r_1. Pošalje $Cert(Boris)$ i r_1 Ani.
2: Ana odabere nasumičan izazov, r_2. Također izračuna $y_1 = sig_{Ana}(ID(Boris)||r_1||r_2)$ i pošalje $Cert(Ana)$, r_2 i y_1 Borisu.
3: Boris verificira Anin javni ključ, ver_{Ana}, na certifikatu $Cert(Ana)$. Nakon toga provjeri: $ver_{Ana}(ID(Boris)||r_1||r_2, y_1) = true$. Ako je to istina, tada Boris "prihvaća", a u suprotnom "odbija". Boris također izračuna $y_2 = sig_{Boris}(ID(Ana)||r_2)$ i pošalje y_2 Ani.

Algoritam 6 je tipična međusobna identifikacijska shema u postavkama javnoga ključa. Može se dokazati da je siguran ako je potpisna shema sigurna i ako su izazovi generirani nasumično. Slika 4.1 ilustrira shemu, izostavljajući slanje certifikata Ane i Borisa. Na toj slici i nadalje, s "A" ćemo označavati "ID(Ana)", a sa "B" ćemo označavati "ID(Boris)".

Sljedeći teorem navodi sigurnost Algoritma 6 kao funkciju sigurnosti temeljne potpisne sheme (gdje je sigurnost potpisne sheme opisana koristeći notaciju sličnu kao i kod MAC-ova).

Teorem 4.1. *Pretpostavimo da je sig (ϵ, Q)-sigurna potpisna shema, i pretpostavimo da je nasumičan izazov dužine k bitova. Tada je Algoritam 6 $(\frac{Q}{2^{k-1}} + 2\epsilon, Q)$-sigurna međusobna identifikacijska shema.*

Ana		Boris
	$\xleftarrow{r_1}$	
$y_1 = sig_A(B\|\|r_1\|\|r_2)$		
	$\xrightarrow{r_2, y_1}$	
		$ver_A(B\|\|r_1\|\|r_2, y_1) = true?$ $y_2 = sig_B(A\|\|r_2)$
	$\xleftarrow{y_2}$	
$ver_B(A\|\|r_2, y_2) = true?$		

Slika 4.1: Tok informacija u Algoritmu 6.

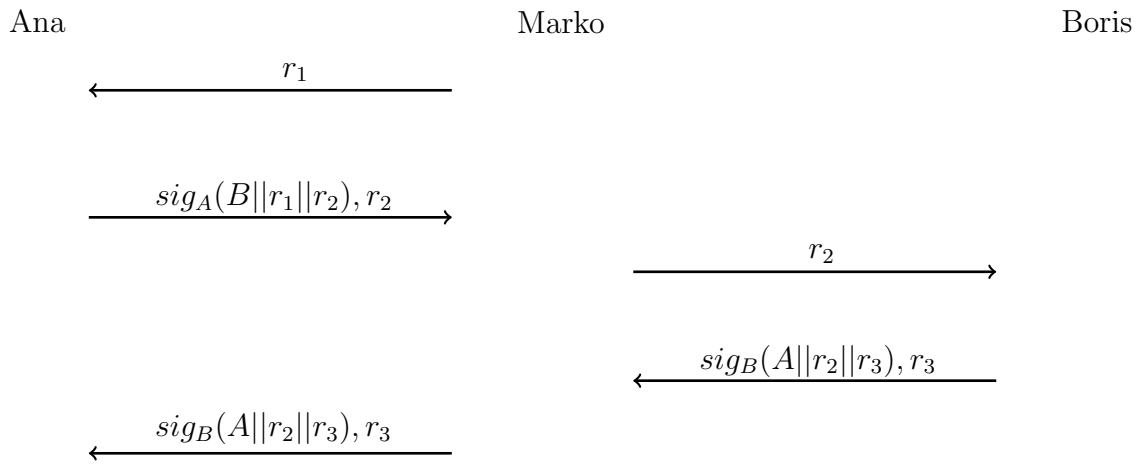
Napomena 4.1. *U Teoremu 4.1, broj prethodnih sesija je Q, dok je u Teoremu 3.1, broj prethodnih sesija bio ograničen na $\frac{Q}{2}$. U Algoritmu 6 Ana i Boris koriste različite ključeve, te je prevarantu dozvoljeno da vidi Q potpisa posebno kreiranih od Ane i od Borisa. S druge strane, u Algoritmu 4, i Ana i Boris koriste iste ključeve da kreiraju MAC-ove. S obzirom da želimo ograničiti prevaranta da vidi Q MAC-ova kreiranih s bilo kojim ključem, zbog toga smo prisiljeni tražiti da je prevarantu dozvoljeno prisluškivati najviše $\frac{Q}{2}$ prethodnih sesija.*

Poučno je razmotriti različite modifikacije ove sheme. Neke modifikacije ispadnu nesigurne dok druge budu sigurne. Primjer nesigurne (modificirane) sheme uključuje treći nasumičan broj r_3 koji je potpisan od strane Borisa; s ovom modifikacijom, shema postaje ranjiva na paralelni sesijski napad. Shema je prikazana Algoritmom 7.

Algoritam 7 ((Nesigurna) Međusobna autentikacija javnim ključem)

1: Boris odabere nasumičan izazov, r_1. Nakon toga pošalje $Cert(Boris)$ i r_1 Ani.
2: Ana odabere nasumičan izazov, r_2. Ona također izračuna $y_1 = sig_{Ana}(ID(Boris)||r_1||r_2)$ i pošalje $Cert(Ana)$, r_2 i y_1 Borisu.
3: Boris verificira Anin javni ključ, ver_{Ana}, na certifikatu $Cert(Ana)$. Nakon toga provjeri: $ver_{Ana}(ID(Boris)||r_1||r_2, y_1) = true$. Ako je to istina, Boris "prihvaća", a u suprotnom "odbija". Boris također odabere nasumičan broj r_3, izračuna: $y_2 = sig_{Boris}(ID(Ana)||r_2||r_3)$ i pošalje r_3 i y_2 Ani.
4: Ana verificira Borisov javni ključ, verBoris, na certifikatu $Cert(Boris)$. Zatim provjeri ako je: $ver_{Boris}(ID(Ana)||r_2||r_3, y_2) = true$. Ako je to istina, Ana "prihvaća", a u suprotnom "odbija".

U Algoritmu 7, nasumična vrijednost, r_3, odabrana je i potpisana od strane Borisa (zajedno s r_2) u trećem toku sheme. Ovaj dodatni dio informacije u potpisu, čini shemu nesigurnom zato što je potpis u trećem toku konstruiran na sličan način kao potpis u drugom toku. To omogućava da se provede paralelan sesijski napad opisan na Slici 4.2. U tom napadu, Marko inicira sesiju s Anom, pretvarajući se da je Boris. Nakon toga inicira drugu sesiju, s Borisom, pretvarajući se da je Ana. Zatim, Borisov odgovor u drugom toku druge sesije proslijedi Ani u trećem toku prve sesije.



Slika 4.2: Napad na Algoritam 7.

5 Schnorrova identifikacijska shema

Drugi pristup identifikacijskoj shemi je dizajniranje sheme "od nule", bez korištenja nekih drugih kriptografskih alata kao "sastavnih komponenti". Potencijalna prednost shema ovoga tipa je da mogu biti efikasnije i imati manju komunikacijsku kompleksnost od shema iz prethodnih poglavlja. Takve sheme tipično uključuju da se neko identificira dokazujući da zna odgovor na neku tajnu vrijednost (npr. tajni ključ), a da ne moraju otkriti tu vrijednost. Schnorrova identifikacijska shema (Algoritam 8) je primjer takve sheme.

Algoritam 8 (Schnorr identifikacijska shema)

1: Ana odabere nasumičan broj, k, gdje je $0 \leq k \leq q-1$, i izračuna $\gamma = \alpha^k \bmod p$. Zatim pošalje $Cert(Ana)$ i γ Borisu.
2: Boris verificira Anin javni ključ, v, na certifikatu $Cert(Ana)$. Boris odabere nasumičan izazov r, gdje je $1 \leq r \leq 2^t$, i pošalje r nazad Ani.
3: Ana izračuna $y = k + ar \bmod q$ i pošalje odgovor y Borisu.
4: Boris verificira $\gamma \equiv \alpha^y v^r \pmod p$. Ako je kongruencija točna, onda Boris "prihvaća"; u suprotnom Boris "odbija".

Ova shema je bazirana na problemu diskretnog logaritma. Uzmimo da je α element prostog reda q u grupi $\mathbb{Z}_p^*$ (gdje je p prost i $p-1 \equiv 0 \pmod q$). Tada je $\log_\alpha \beta$ definiran za svaki element $\beta \in \langle \alpha \rangle$, i $0 \leq log_\alpha \beta \leq q-1$. Da bi postavku smatrali sigurnom, specificirat ćemo da je $p \approx 21024$ i $q \approx 2160$.

Shema zahtjeva sustav nadležnosti, to jest TA, koji odabire neke zajedničke sistemske parametre (domenske parametre) za shemu, kao što su sljedeći:

1. p je velik prost broj (npr. $p \approx 21024$).
2. q je velik djelitelj prostog broja $p-1$ (npr. $q \approx 2160$).
3. $\alpha \in \mathbb{Z}_p^*$ je reda q.
4. t je sigurnosni parametar takav da je $q > 2^t$. (Vjerojatnost prevaranta da će prevariti Anu ili Borisa će biti 2^{-t}, dakle $t = 40$ će pružiti adekvatnu zaštitu za većinu praktičnih aplikacija.)

Parametri domene p, q, α i t su javni, i bit će korišteni od strane svakoga tko se nalazi u mreži. Svaki korisnik unutar mreže odabire svoj privatni ključ, a, gdje je $0 \leq a \leq q-1$, i konstruira odgovarajući javni ključ $v = \alpha^{-a} \bmod p$. Primjetimo da v može biti izračunat kao $(\alpha^a)^{-1} \bmod p$, ili (još efikasnije) kao $\alpha^{q-a} \bmod p$. TA izdaje certifikate za svakoga u

mreži. Svaki korisnički certifikat će sadržavati njihov javni ključ (i, možda, javne parametre domene). Ova informacija, kao i korisnikova identifikacijska informacija, potpisana je od strane TA. Sljedeće kongruencije demonstriraju da će Ana moći dokazati svoj identitet Borisu, pretpostavljajući da su obje stranke iskrene i da korektno računaju:

$$\begin{aligned}
\alpha^y v^r &\equiv \alpha^{k+ar} v^r \pmod{p} \\
&\equiv \alpha^{k+ar} \alpha^{-ar} \pmod{p} \\
&\equiv \alpha^k \pmod{p} \\
&\equiv \gamma \pmod{p}
\end{aligned}$$

Činjenica da će Boris prihvatiti Anin dokaz identiteta (pretpostavljajući da su on i Ana iskreni) se ponekad naziva potpuno svojstvo sheme.

Sljedeći primjer izostavlja autentikaciju Aninog javnog ključa od strane Borisa.

Primjer 5.1. *Pretpostavimo da je* $p = 88667$, $q = 1031$ *i* $t = 10$. *Element* $\alpha = 70322$ *je reda* q *u* $\mathbb{Z}_p^*$. *Pretpostavimo da je Anin privatni ključ* $a = 755$. *Tada imamo sljedeće:*

$$\begin{aligned}
v &= \alpha^{-a} \pmod{p} \\
&= 70322^{1031-755} \pmod{88667} \\
&= 13136.
\end{aligned}$$

Sada pretpostavimo da je Ana odabrala nasumičan broj $k = 543$. *Nakon toga izračuna:*

$$\begin{aligned}
\gamma &= \alpha^k \pmod{p} \\
&= 70322^{543} \pmod{88667} \\
&= 84109
\end{aligned}$$

i pošalje γ *Borisu. Pretpostavimo da Boris pošalje izazov* $r = 1000$. *Tada Ana izračuna:*

$$\begin{aligned}
y &= k + ar \pmod{q} \\
&= 543 + 755 \cdot 1000 \pmod{1031} \\
&= 851
\end{aligned}$$

i pošalje y *Borisu kao njezin odgovor. Boris tada verificira:*

$$84109 \equiv 70322^{851} 13136^{1000} \pmod{88667}.$$

I u konačnici Boris "prihvaća".

Schnorr-ova identifikacijska shema je dizajnirana da bude brza i efikasna, s oba pogleda, računalnog i količinskog (broj informacija koje trebaju biti izmjenjene unutar sheme). Također je dizajnirana da minimizira količinu računanja od strane Ane. To je poželjno zato što u većini praktičnih aplikacija Anini izračuni će biti obavljeni od strane pametne kartice (smart card) s malom računalnom snagom, dok će Borisovo računanje biti obavljeno od strane mnogo snažnijeg računala.

Promotrimo malo Anino računanje. Korak 1 zahtjeva računanje eksponenciranja (mod p). Korak 3 sadrži jedno zbrajanje i jedno množenje (mod p). Modularno eksponenciranje je računalno zahtjevna operacija, ali ovo može biti unaprijed izračunato offline, prije nego je shema izvršena, ako je potrebno. Online računanja koja Ana treba izračunati su vrlo skromna.

Jednostavno je izračunati broj bitova koji su preneseni tokom sheme. Informacije koje su prenesene (bez Aninog certifikata) prikazane su na Slici 5.1. U tom dijagramu, oznaka $\in_R$ korištena je za označavanje nasumičnog odabira napravljenog od određenog skupa.

Ana		Boris
$k \in_R \{0, \ldots, q-1\}$		
$\gamma = \alpha^k \pmod p$		
	$\xrightarrow{\gamma \text{ (1024 bitova)}}$	
	$\xleftarrow{r \text{ (40 bitova)}}$	$r \in_R \{1, \ldots, 2^t\}$
$y = k + ar \pmod q$	$\xrightarrow{y \text{ (160 bitova)}}$	
		$\gamma \equiv \alpha^y v^r \pmod p$?

Slika 5.1: Tok informacija u Algoritmu 8.

Ana pošalje Borisu 1024 bita informacije (bez njezinog certifikata) u prvom toku. Boris pošalje Ani 40 bitova u drugom toku i Ana pošalje 160 bitova Borisu u trećem toku. Iz toga možemo zaključiti da su i komunikacijski zahtjevi prilično skromni.

Informacije poslane u drugom i trećem toku sheme su reducirane na način na koji je shema dizajnirana. U drugom toku, izazov može biti bilo koji broj između 0 i $q-1$; to bi imalo 160-bitni izazov, a 40-bitni izazov već pruža dovoljnu sigurnost za većinu aplikacija. U trećem toku, vrijednost y je eksponent. Ta vrijednost je samo 160 bitova dugačka zato što shema radi unutar podgrupe od $\mathbb{Z}_p^*$ reda $q \approx 2160$. To dopušta da prijenos informacija u trećem toku bude znatno reduciran, u usporedbi s implementacijom sheme u "cijeloj grupi", $\mathbb{Z}_p^*$, u kojoj je eksponent 1024 bita dug.

Prvi tok očigledno zahtjeva prosljeđivanje najviše informacija. Jedan način na koji je moguće reducirati količinu informacije je zamjena 1024-bitne vrijednosti γ sa 160-bitnom sažetom porukom, $\gamma^{'} = SHA-1(\gamma)$. Tada bi u zadnjem koraku sheme Boris verificirao sažetu poruku $\gamma^{'} = SHA-1(\alpha^y v^r (\text{mod } p))$.

5.1 Sigurnost Schnorrove identifikacijske sheme

Proučimo sigurnost Schnorrove identifikacijske sheme. Kao što smo rekli već prije, t je sigurnosni parametar. Dovoljno je velik da bi mogao spriječiti prevaranta koji se predstavlja da je Ana (recimo Ivana), od pogađanja Borisovog izazova, r. (Ako bi Ivana pogodila točnu vrijednost r, mogla bi odabrati bilo koju vrijednost za y i unaprijed izračunati

$$\gamma = \alpha^v v^r \pmod p$$

Dala bi Borisu vrijednost γ u prvom toku sheme, i kada bi primila izazov r, odgovorila bi Borisu s vrijednošću y koju je već odabrala. Tada bi kongruencija koja uključuje γ bila verificirana od strane Borisa, i on bi "prihvatio". Vjerojatnost da bi Ivana pogodila vrijednost r iznosi točno 2^{-t} ako je r odabran nasumično od strane Borisa. Primjetimo da svaki put kada se Ana identificira Borisu, on bi trebao odabrati novi nasumični izazov, r. Ako bi Boris uvijek koristio isti izazov r, tada bi se Ivana mogla predstavljati kao Ana metodom koju smo upravo opisali. Anini izračuni unutar sheme uključuju korištenje njezinog privatnog ključa, a. Vrijednost a funkcionira poput PIN-a, i zbog toga uvjerava Borisa da je osoba koja provodi identifikacijsku shemu uistinu Ana. Ali postoji bitna razlika naspram PIN-a: u ovoj identifikacijskoj shemi, vrijednost od a nije otkrivena. Umjesto toga, Ana (ili preciznije, Anina pametna kartica) "dokaže" da zna vrijednost od a u trećem toku sheme, izračunajući točan odgovor, y, na izazov, r, poslan od strane Borisa. Prevarant bi mogao pokušati izračunati a, zato što je a samo diskretan logaritam poznate veličine: $a = -\log_\alpha v$ u $\mathbb{Z}_p^*$. Međutim, mi pretpostavljamo da je to izračunavanje nemoguće.

Tvrdili smo da Ivana može pogoditi Borisov izazov r, i tako se predstaviti kao Ana, s vjerojatnošću 2^{-t}. Pretpostavimo da Ivana može učiniti to s još većom vjerojatnošću.

Ako bi se Ivana mogla predstaviti kao Ana uspješno s vjerojatnošću većom od 2^{-t}, tada je vjerojatno da Ivana zna neki γ (vrijednost njezinog izbora), i dva moguća izazova, r_1 i r_2, tako da može izračunati odgovore y_1 i y_2, odnosno natjerati Borisa da prihvati. Ako bi Ivana mogla izračunati točan odgovor na jedan izazov za svaki γ, tada bi njezina vjerojatnost uspjeha bila samo 2^{-t}. Pa pretpostavimo da Ivana zna (ili može izračunati) vrijednost r_1, r_2, y_1 i y_2 takve da:

$$\gamma \equiv \alpha^{y_1} v^{r_1} \equiv \alpha^{y_2} v^{r_2} \pmod{p}.$$

Iz toga slijedi:

$$\alpha^{y_1 - y_2} \equiv v^{r_2 - r_1} \pmod{p}.$$

Znamo da je $v \equiv \alpha^{-a} \pmod{p}$, gdje je a Anin privatni ključ. Stoga imamo:

$$\alpha^{y_1 - y_2} \equiv \alpha^{-a(r_2 - r_1)} \pmod{p}.$$

Element α je reda q, pa vrijedi sljedeće:

$$y_1 - y_2 \equiv a(r_1 - r_2) \pmod{q}.$$

Sada imamo $0 < |r_2 - r_1| < 2^t$ i $q > 2^t$ je prost. Odatle je $gcd(r_2 - r_1, q) = 1$, i zbog toga $(r_2 - r_1)^{-1} \bmod q$ postoji. Stoga Ivana može izračunati Anin privatni ključ a na sljedeći način:

$$a = (y_1 - y_2)(r_1 - r_2)^{-1} \pmod{p}.$$

Gornja analiza sugerira da svatko tko je u mogućnosti uspješno se predstavljati kao Ana s vjerojatnošću većom od 2^{-t} mora znati (ili moći lako izračunati) Anin privatni ključ a. Gore smo dokazali da "uspješan" varalica može izračunati a. Suprotno, očito je da bilo tko, tko zna vrijednost od a može oponašati Anu, s vjerojatnošću jednakom 1. Prema tome slijedi, da je biti u mogućnosti oponašati Anu ekvivalentno znanju Aninog privatnog ključa. To svojstvo često nazivamo zvučnost (soundness).

Definicija 5.1. *Kažemo da je shema potpuna ako za danog iskrenog dokazivača i iskrenog verifikatora protokol prolazi s velikom vjerojatnošću. Definicija velike vjerojatnosti ovisi o primjeni, ali općenito podrazumijeva da je vjerojatnost neuspjeha zanemariva.*

Definicija 5.2. *Kažemo da je shema zvučna ako postoji očekivani vremenski polinomijalan algoritam sa sljedećim svojstvom: ako neiskrena osoba (koja se lažno predstavlja) može sa nezanemarivom vjerojatnošću uspješno provesti shemu sa željenom osobom, tada algoritam možemo iskoristiti za izvlačenje dokazivačevog znanja koje s velikom vjerojatnošću dozvoljava uspješno izvršavanje sljedeće sheme.*

Identifikacijsku shemu koja je i zvučna i potpuna nazivamo dokazom znanja (proof of knowledge). Dosadašnje analize utvrdile su da je Schnorrova identifikacijska shema dokaz znanja. Pružit ćemo primjer kako bi ilustrirali gornju diskusiju.

Primjer 5.2. *Pretpostavimo da imamo iste parametre kao u Primjer 5.1.:* $p = 88667$, $q = 1031$ *i* $t = 10$, $\alpha = 70322$ *i* $v = 13136$. *Pretpostavimo da je za* $\gamma = 84109$ *Ivana u mogućnosti nekako odrediti dva točna odgovora:* $y_1 = 851$ *je točan odgovor za izazov* $r_1 = 1000$*; i* $y_2 = 454$ *je točan odgovor na izazov* $r_2 = 19$. *Drugim riječima:*

$$84109 \equiv \alpha^{851} v^{1000} \equiv \alpha^{454} v^{19} \pmod{p}$$

Tada Ivana može izračunati:

$$a = (851 - 454)(1000 - 19)^{-1} \pmod{1031} = 755,$$

i na taj način otkriti Anin privatni ključ.

Dokazali smo da je shema dokaz znanja. Ali to nije dovoljno da budemo sigurni da je shema "sigurna". Još uvijek trebamo uzeti u obzir vjerojatnost da je tajna informacija (Anin privatni ključ) iscurila do ovjeritelja koji je dio sheme, ili promatrača. (To se može smatrati fazom prikupljanja podataka za napad). Mi se nadamo da bilo kakva informacija o a neće doći do Ivane kada Ana dokazuje svoj identitet. Ako je to točno, tada Ivana neće biti u mogućnosti kasnije se maskirati kao Ana (pod pretpostavkom da je izračunavanje diskretnog logaritma od a nemoguće).
Generalno, mogli bismo zamisliti situaciju gdje Ana dokazuje svoj identitet Ivani, na nekoliko različitih načina. Nakon nekoliko sesija sheme, Ivana će pokušati utvrditi vrijednost od a da bi kasnije mogla oponašati Anu. Ako Ivana ne može odererditi nikakvu informaciju o vrijednosti a sudjelovanjem u "razumnom" broju sesija sheme kao verifikator, a zatim provođenjem "razumne" količine računanja, tada se shema naziva Identifikacijska shema bez znanja (zero-kowledge identification sheme). To bi dokazalo da je shema sigurna, pod pretpostavkom da je a nemoguće izračunati. (Naravno, potrebno je definirati, na precizan način, značenje od "razumno", da bi imali smislenu izjavu o sigurnosti.) Pokazat ćemo da je Schnorrova identifikacijska shema identifikacijska shema bez znanja za iskrene verifikatore, gdje je iskren verifikator definiran kao onaj koji odabire svoj izazov r nasumično, kako je specificirano od strane sheme.
Potreban nam je pojam transkirpt (prepiska ili prijepis) sesije, koji je uređena trojka $T = (\gamma, r, y)$ gdje je $\gamma \equiv \alpha^y v^r \pmod{p}$. Verifikator (ili promatrač) može dobiti prijepis $T(S)$ od svake sesije S. Skup mogućih prepisa je:

$$\tau = \{(\gamma, r, y) : 1 \leq r \leq 2^t, 0 \leq y \leq q - 1, \gamma \equiv \alpha^y v^r \pmod{p}\}.$$

Lako je vidjeti da $|\tau| = q2^t$. Nadalje, nije teško dokazati da je vjerojatnost da se bilo koji prijepis pojavljuje u bilo kojoj danoj sesiji $\frac{1}{(q2^t)}$, pod pretpostavkom da su izazovi r generirani nasumično. Argumentiramo to na sljdeći način: za bilo koju fiksnu vrijednost r, postoji veza 1 prema 1 između vrijednosti $\gamma \in \langle\alpha\rangle$ i vrijednost od $y \in 0, \ldots, q-1$ za određeni prijepis. Pretpostavljamo da Ana odabere γ nasumično (tako da odabere nasumičan k i izračuna $\gamma = \alpha^k \bmod p$), i također pretpostavimo da Boris odabere r nasumično (zato što je on iskren verifikator). Ove dvije vrijednosti odlučuju vrijednost od y. Pošto postoji q mogućih odabira za γ i 2^t mogućih odabira za r, slijedi da se svaki mogući prijepis dogodi sa istom vjerojatnošću, $\frac{1}{(q2^t)}$, u sesijama u kojima postoji iskren verifikator.
Ključna stvar identifikacijske sheme bez znanja je svojstvo zvano simulativnost. Ispostavlja se da Ivana (ili bilo ko drugi) može generirati simulirani prijepis, koji ima točno istu vjerojatnosnu distribuciju kao pravi prijepis, bez da ima uvid u shemu. To se napravi prateći sljedeća tri koraka:

1. odaberi $r \in_R 1, \ldots, 2^t$
2. odaberi $y \in_R 0, \ldots, q-1$
3. $\gamma = \alpha^y v^r \pmod p$.

Lako se vidi da je vjerojatnost da je bilo koji T $\in \tau$ generiran s procedurom iznad jednaka $\frac{1}{(q2^t)}$. Stoga, vrijedi:

$$\mathbf{Pr}_{real}[T] = \mathbf{Pr}_{sim}[T] = \frac{1}{q2^t}$$

za svaki $T \in \tau$, gdje je $\mathbf{Pr}_{real}[T]$ vjerojatnost generiranja prijepisa T tokom prave sesije, i $\mathbf{Pr}_{sim}[T]$ vjerojatnost generiranja T kao simuliranog prijepisa.

Koja je značajnost činjenice da prijepis može biti simuliran? Tvrdimo da, što god iskren verifikator može izračunati nakon sudjelovanja u nekoliko sesija sheme, verifikator može alternativno izračunati istu informaciju bez sudjelovanja u sesiji sheme. Posebno, računanje Aninog privatnog ključa, a, koji je nužan za Ivanu da bi mogla oponašati Anu, nije olakšano Ivani ako ona igra ulogu verifikatora u jednoj ili više sesija u kojima odabire izazove nasumično.

Ranije navedene tvrdnje ćemo obrazložiti u nastavku. Pretpostavimo da postoji algoritam EXTRACT koji za dani skup prijepisa, $T_1, \ldots, T_l$, računa privatni ključ, a, sa vjerojatnošću ϵ. Pretpostavljmo da su prijepisi pravi prijepisi sesija, u kojima učesnici slijede shemu. Pretpostavimo da su $T_1^{'}, \ldots, T_l^{'}$ simulirani prijepisi. Primjetili smo da je vjerojatnosna distribucija na simuliranim prijepisima identična vjerojatnosnoj distribuciji na pravim

prijepisima. Stoga EXTRACT $(T_1^{'}, \ldots, T_l^{'})$ će računati a s vjerojatnošću ϵ. To povlači da izvođenje sheme ne olakšava računanje a, pa je shema Identifikacijska shema bez znanja.

Razmislimo o vjerojatnosti da Ivana ("neiskren verifikator") može prikupiti neke korisne informacije odabirom izazova r na ne-uniforman način. Preciznije, pretpostavimo da Ivana odabere izazov r koristeći neku funkciju koja ovisi, na kompliciran način, o Aninom odabiru γ. Ne postoji način na koji bi perfektno simulirali konačnu vjerojatnosnu distribuciju prijepisa, i stoga ne možemo dokazati da je shema Identifikacijska shema bez znanja na način na koji smo to napravili za iskrenog verifikatora. Naglasimo da ne postoji poznat napad na shemu baziran na pravljenju nenasumičnih izazova; samo želimo reći da tehnika koju smo korisitili prije za dokaz ne može biti primjenjena u ovom slučaju. Jedini poznati dokazi za sigurnost sheme za proizvoljne verifikatore zahtijevaju dodatne pretpostavke.

Interaktivna shema je dokaz znanja ukoliko je nemoguće oponašati Anu bez znanja vrijednosti Aninog ključa. To znači da je jedini način za "probijanje" sheme zapravo računanje a. Za shemu ćemo reći da je identifikacijska shema bez znanja ako ne otkriva informacije o Aninom privatnom ključu, to jest računanje Aninog privatnog ključa nije olakšano sudjelovanjem u shemi (u Borisovoj ulozi verifikatora) u nekom određenom broju sesija. Ako je shema identifikacijska shema bez znanja dokaz znanja, onda je "sigurna".

6 Okamotova identifikacijska shema

U ovom poglavlju, objasnit ćemo modificiranu Schnorrovu identifikacijsku shemu nazvanu po Okamotu. Možemo dokazati da je ova modifikacija sigurna, pod pretpostavkom da je gotovo nemoguće za osobu koja pokušava probiti shemu doći do načina kako se izračunava diskretni logaritam u $\mathbb{Z}_p^*$.

Algoritam 9 (Okamoto indetifikacijska shema)

1: Ana odabere nasumičan broj k_1, k_2, gdje $0 \leq k_1$, $k_2 \leq q-1$, i izračuna $\gamma = \alpha_1^{k_1}\alpha_2^{k_2} \bmod p$.
2: Ana pošalje certifikat, $Cert(Ana) = (ID(Ana), v, s)$, i γ Borisu.
3: Boris verificira $ver_{TA}(ID(Ana)||v, s) = true$.
4: Boris odabere nasumičan broj r, $1 \leq r \leq 2^t$, i pošalje ga Ani.
5: Ana izračuna $y_1 = k_1 + a_1 r \bmod q$ i $y_2 = k_2 + a_2 r \bmod q$ i pošalje y_1 i y_2 Borisu.
6: Boris verificira: $\gamma \equiv \alpha_1^{y_1}\alpha_2^{y_2}v^r \pmod p$.

Za postavku sheme, TA odabere p i q u Schnorr identifikacijskoj shemi. TA također odabere dva elementa α_1, $\alpha_2 \in \mathbb{Z}_p^*$ oba reda q. Kako je $\mathbb{Z}_p^*$ ciklička grupa, slijedi da ima jedinstvenu podgrupu H reda q, koja je ciklička i bilo koji element reda q iz $\mathbb{Z}_p^*$ je generator grupe H. Stoga $\alpha_1 \in \langle\alpha_2\rangle$ i $\alpha_2 \in \langle\alpha_1\rangle$. Označimo $c = \log_{\alpha_1}\alpha_2$. Vrijednost od c je tajna za sve učesnike (uključujući Anu). Pretpostavljamo da je nemoguće za bilo koga da izračuna vrijednost od c. Anin javni ključ v se računa na sljedeći način:

$$v = \alpha_1^{-a_1}\alpha_2^{-a_2} \pmod p,$$

gdje a_1 i a_2 sadrže Anin privatni ključ. Okamotova identifikacijska shema prikazana u Algoritmu 9 ilustrirana je sljedećim primjerom:

Primjer 6.1. *Kao i u prethodnim primjerima, uzet ćemo da je $p = 88667$, $q = 1031$ i $t = 10$. Pretpostavimo da je $\alpha_1 = 58902$ i $\alpha_2 = 73611$ (α_1 i α_2 su reda q u $\mathbb{Z}_p^*$). Recimo da su $a_1 = 846$ i $a_2 = 515$; tada je $v = 13078$. Pretpostavimo da Ana odabere $k_1 = 899$ i $k_2 = 16$; tada je $\gamma = 14574$. Ako Boris pošalje izazov $r = 489$ tada će Ana odgovoriti s $y_1 = 131$ i $y_2 = 287$. Boris će verificirati da je:*

$$58902^{131}73611^{287}13078^{489} \equiv 14574 \pmod{88667}.$$

Pa Boris prihvaća Anin dokaz identiteta.

Glavna razlika između Okamotove i Schnorrove sheme je da možemo dokazati da je Okamotova identifikacijska shema sigurna pod uvjetom da izračun diskretnog logaritma $\log_{\alpha_1}\alpha_2$

nije jednostavan.

Dokaz sigurnosti je jednostavan. Skica dokaza ide ovako: Pretpostavimo da se Ana identificirala Ivani polinomijalno mnogo puta izvršavajući shemu. Zatim pretpostavimo da Ivana može saznati neke informacije o vrijednosti Aninih tajnih eksponenata a_1 i a_2. Ako je to istina, tada možemo pokazati (s velikom vjerojatnošću) da Ana i Ivana zajedno mogu izračunati diskretan logaritam c u polinomijalnom vremenu. S obzirom da je to kontradikcija s početnom pretpostavkom, dokazali smo da Ivana nije u mogućnosti dobiti informacije o Aninim eksponentima sudjelujući u shemi.

Prvi dio ove procedure sličan je dokazu Schnorrove identifikacijske sheme. Pretpostavimo da Ivana zna vrijednost γ za koju može izračunati pravi odgovor na dva različita izazova, r i s. To jest pretpostavimo da Ivana može izračunati y_1, y_2, z_1, z_2, r i s gdje je $r \neq s$ i

$$\gamma \equiv \alpha_1^{y_1}\alpha_2^{y_2}v^r \equiv \alpha_1^{z_1}\alpha_2^{z_2}v^s \pmod{p}.$$

Ivana može postaviti

$$b_1 = (y_1 - z_1)(r - s)^{-1} \pmod{q}$$

i

$$b_2 = (y_2 - z_2)(r - s)^{-1} \pmod{q}.$$

Tada je lako provjeriti da li je:

$$v \equiv \alpha_1^{-b_1}\alpha_2^{-b_2} \pmod{p}.$$

U nastavku ćemo pokazati kako Ana i Ivana zajedno mogu izračunati vrijednost c (s velikom vjerojatnošću). Pretpostavimo da je Ivana u mogućnosti odrediti vrijednosti b_1 i b_2 takve da je:

$$v \equiv \alpha_1^{-b_1}\alpha_2^{-b_2} \pmod{p}.$$

Nadalje pretpostavimo da je Ana otkrila tajne vrijednosti a_1 i a_2 Ivani. Pa imamo:

$$v \equiv \alpha_1^{-a_1}\alpha_2^{-a_2} \pmod{p},$$

stoga treba vrijediti:

$$\alpha_1^{a_1-b_1} \equiv \alpha_2^{b_2-a_2} \pmod{p}.$$

Pretpostavimo da je $(a_1, a_2) \neq (b_1, b_2)$. Tada $(b_2 - a_2)^{-1} \bmod q$ postoji, i diskretni logaritam

$$c = \log_{\alpha_1} \alpha_2 = (a_1 - b_1)(b_2 - a_2)^{-1} \pmod{q}.$$

može biti izračunat u polinomijalnom vremenu.
Ostaje još za razmotriti mogućnost da je $(a_1, a_2) = (b_1, b_2)$. Ako je to istina, tada vrijednost od c ne može biti izračunata na prethodno prikazani način. Vjerojatnost da je $(a_1, a_2) = (b_1, b_2)$ jednaka je $\frac{1}{q}$ što je vrlo malo, pa će stoga procedura gdje Ana i Ivana računaju c gotovo sigurno uspjeti.

Definirajmo:

$$\mathcal{A} = \{(a_1', a_2') \in \mathbb{Z}_q \times \mathbb{Z}_q : \alpha_1^{-a_1'}\alpha_2^{-a_2'} \equiv \alpha_1^{-a_1}\alpha_2^{-a_2} \pmod{p}\}.$$

$\mathcal{A}$ sadrži sve moguće uređene parove koji mogu biti Anini tajni eksponenti. Primjetimo da je

$$\mathcal{A} = \{(a_1 - c\theta, a_2 + \theta) : \theta \in \mathbb{Z}_q\},$$

gdje je $c = \log_{\alpha_1} \alpha_2$, što znači da $\mathcal{A}$ sadrži q uređenih parova. Uređeni par (b_1, b_2) izračunat od strane Ivane je sigurno unutar skupa $\mathcal{A}$. Tvrdimo da je vrijednost para (b_1, b_2) neovisna o vrijednosti para (a_1, a_2) koji sadrži Anine tajne eksponente. Pošto je (a_1, a_2) odabran nasumično od strane Ane, vjerojatnost da je $(a_1, a_2) = (b_1, b_2)$ jednaka je $\frac{1}{q}$.

Objasnimo što znači da je (b_1, b_2) "neovisno" o (a_1, a_2).
Ideja je da je Anin par (a_1, a_2) jedan od q mogućih uređenih parova u skupu $\mathcal{A}$, i Ana nije otrkrila informaciju koji je pravi uređeni par identificirajući se Ivani. Neformalno rečeno, Ivana zna da uređeni par iz $\mathcal{A}$ sadrži Anine eksponente, ali ne može reći koji točno. Promotrimo informaciju koja se razmjenjuje tijekom indetifikacijske sheme. U svakoj izvedbi sheme, Ana odabere γ; Ivana odabere r, i Ana otkrije y_1 i y_2 tako da vrijedi:

$$\gamma \equiv \alpha_1^{y_1}\alpha_2^{y_2}v^r \pmod{p}.$$

Prisjetimo se da Ana računa:

$$y_1 = k_1 + a_1 r \pmod{q}.$$

i

$$y_2 = k_2 + a_2 r \pmod{q}.$$

gdje je:

$$\gamma = \alpha_1^{k_1}\alpha_2^{k_2} \pmod{p}.$$

Ali primjetimo da k_1 i k_2 nisu otkriveni (a samim time ni a_1 i a_2). Određena četvorka (γ, r, y_1, y_2) koja je generirana tokom jednog izvođenja sheme je naizgled ovisna o Aninom uređenom paru (a_1, a_2), pošto su y_1 i y_2 definirani pomoću a_1 i a_2. Ali dokazat ćemo da svaka takva četvorka može biti jednako generirana iz bilo kojeg uređenog para $(a_1', a_2') \in \mathcal{A}$.

Da bi to razumjeli, pretpostavimo da su $(a_1', a_2') \in \mathcal{A}$, to jest $a_1' = a_1 - c\theta$ i $a_2' = a_2 + \theta$, gdje je $0 \leq \theta \leq q-1$. Možemo izraziti y_1 i y_2 na sljedeći način:

$$\begin{aligned} y_1 &= k_1 + a_1 r \\ &= k_1 + (a_1' + c\theta)r \\ &= (k_1 + rc\theta) + a_1' r, \end{aligned}$$

i

$$\begin{aligned} y_2 &= k_2 + a_2 r \\ &= k_2 + (a_2' - \theta)r \\ &= (k_2 - r\theta) + a_2' r, \end{aligned}$$

gdje je svo računanje odrađeno u $\mathbb{Z}_p$. To znači da je četvorka (γ, r, y_1, y_2) također konzistentna s uređenim parom (a_1', a_2') koristeći nasumične odabire $k_1' = k_1 + rc\theta$ i $k_2' = k_2 - r\theta$ da bi dobili isti γ. Već smo naglasili da vrijednosti k_1 i k_2 nisu otkriveni od strane Ane, pa stoga četvorka (γ, r, y_1, y_2) ne daje informaciju bez obzira koji uređeni par iz $\mathcal{A}$ Ana zapravo koristi za njen tajni eksponent.
Ovaj dokaz sigurnosti je poprilično jednostavan. Bilo bi korisno prisjetiti se svojstava sheme koji vode do dokaza sigurnosti. Osnovna ideja bazirana je na tome da Ana odabere dva tajna eksponenta umjesto jednog. Postoji ukupno q parova u skupu $\mathcal{A}$ koji su "ekvivalentni" Aninom paru (a_1, a_2). Ono što nas dovodi do kontradikcije je činjenica da nas poznavanje dva različita para iz $\mathcal{A}$ dovodi do efikasne metode računanja diskretnog logaritma c. Ana zna jedan par iz $\mathcal{A}$, a pokazali smo da ukoliko Ivana može oponašati Anu tada je Ivana u mogućnosti s velikom vjerojatnošću izračunati par iz $\mathcal{A}$ koji je različit od Aninog para. Stoga Ana i Ivana zajedno mogu pronaći dva para iz $\mathcal{A}$ i izračunati c, što nas dovodi do kontradikcije. Sljedeći primjer ilustrira računanje $log_{\alpha_1}\alpha_2$ od strane Ane i Ivane.

Primjer 6.2. *Kao u Primjeru 6.1 uzet ćemo da je $p = 88667$, $q = 1031$ i $t = 10$, i pretpostaviti da je $v = 13078$. Također a_1, a_2, α_1 i α_2 imaju iste vrijednosti kao i prije. Recimo da je Ivana odlučila da je:*

$$\alpha_1^{131}\alpha_2^{287}v^{489} \equiv \alpha_1^{890}\alpha_2^{303}v^{199} \pmod{p}.$$

Tada može izračunati:

$$b_1 = (131 - 890)(489 - 199)^{-1} \pmod{1031} = 456$$

i

$$b_2 = (287 - 303)(489 - 199)^{-1} \pmod{1031} = 519.$$

Koristeći vrijednosti a_1 i a_2 dobivene od Ane, vrijednost

$$c = (846 - 456)(519 - 515)^{-1} \pmod{1031} = 613$$

je izračunata. Ova vrijednost c je zapravo $\log_{\alpha_1} \alpha_2$, što možemo potvrditi računanjem:

$$58902^{613} \pmod{88667} = 73611.$$

7 Guillou-Quisquaterova identifikacijska shema

U ovom poglavlju opisat ćemo drugu identifikacijsku shemu nazvanu po Guillou i Quisquateru, koja je bazirana na RSA kriptosustavu. Postavka sheme ide ovako: TA odabere dva prosta broja p i q i njihov umnožak $n = pq$. Vrijednosti od p i q su tajne, dok je n javan. Kao što smo već imali, p i q moraju biti dovoljno veliki tako da je faktoriranje n gotovo nemoguće za osobu koja ga pokušava probiti. Također, TA odabere veliki prosti broj b koji će funkcionirati kao sigurnosni parametar i kao javni RSA enkripcijski eksponent. Točnije, pretpostavimo da je b 40-bitni prosti broj takav da je $(b, \varphi(n)) = 1$. Sada Ana odabere broj u, gdje je $0 \leq u \leq n-1$, i izračuna:

$$v = (u^{-1})^b \pmod{n}.$$

Vrijednost od v je dana TA, i tada TA izračuna potpis:

$$s = sig_{TA}(ID(Ana)||v).$$

Tada su $ID(Ana)$, v i s smješteni na Anin certifikat. Brojevi n i b su javni domenski parametri, v je Anin javni ključ i u je Anin privatni ključ. Kada Ana želi dokazati svoj identitet Borisu, izvrši se Algoritam 10.

Algoritam 10 (Guillou-Quisquater identifikacijska shema)

1: Ana odabere nasumični broj k, gdje je $0 \leq k \leq n-1$ i izračuna: $\gamma = k^b \pmod{n}$
2: Ana da Borisu svoj certifikat $Cert(Ana) = (ID(Ana), v, s)$ i γ.
3: Boris verificira $ver_{TA}(ID(Ana)||v, s) = true$.
4: Boris odabere nasumični broj r, $0 \leq r \leq b-1$ i da ga Ani.
5: Ana izračuna $y = ku^r \pmod{n}$ i da y Borisu.
6: Boris verificira $\gamma \equiv v^r y^b \pmod{n}$.

Prikazat ćemo shemu na sljedećem primjeru.

Primjer 7.1. *Pretpostavimo da je TA odabrao $p = 467$ i $q = 479$, pa je $n = 223693$. Pretpostavimo također da je $b = 503$ i Anin tajni broj $u = 101576$. Tada će Ana izračunati:*

$$\begin{aligned} v &= (u^{-1})^b \pmod{n} \\ &= (101576^{-1})^{503} \pmod{223693} \\ &= 89888. \end{aligned}$$

Sada, pretpostavimo da Ana dokazuje svoj identitet Borisu i odabere $k = 187485$ i pošalje

Borisu vrijednost

$$\begin{aligned}\gamma &= k^b \pmod n \\ &= 187485^{503} \pmod{223693} \\ &= 24412.\end{aligned}$$

Recimo da Boris odgovori s izazovom $r = 375$. Tada Ana izračuna

$$\begin{aligned}y &= ku^r \pmod n \\ &= 187485 \cdot 101576^3 75 \pmod{223693} \\ &= 93725\end{aligned}$$

i da y Borisu. Boris tada verificira:

$$24412 \equiv 89888^{375} 93725^{503} \pmod{223693}.$$

Stoga, Boris prihvaća Anin dokaz identiteta.

Dokažimo da je Guillou-Quisquaterova identifikacijska shema zvučna i potpuna. Kao što je inače slučaj, dokazivanje potpunosti je prilično jednostavno:

$$\begin{aligned}v^r y^b &\equiv (u^{-b})^r (ku^r)^b \pmod n \\ &\equiv u^{-br} k^b u^{br} \pmod n \\ &\equiv k^b \pmod n \\ &\equiv \gamma \pmod n.\end{aligned}$$

Obratimo sada pažnju na dokaz zvučnosti. Dokazat ćemo da je shema zvučna ako pokažemo da je nemoguće izračunati u iz v. Pošto je v formirano od u RSA enkripcijom, to je uvjerljiva pretpostavka. Pretpostavimo da Ivana zna vrijednost γ za koju ima vjerojatnost $\epsilon \geq \frac{2}{b}$ da uspješno oponaša Anu u verifikacijskoj shemi. Za γ razumno je pretpostaviti da Ivana može izračunati vrijednost y_1, y_2, r_1, r_2 gdje je $r_1 \neq r_2$ tako da je

$$\gamma \equiv v^{r_1} y_1^b \equiv v^{r_2} y_2^b \pmod n.$$

Pretpostavimo bez gubitka općenitosti da je $r_1 > r_2$. Tada imamo:

$$v^{r_1 - r_2} \equiv \left(\frac{y_2}{y_1}\right)^b \pmod n.$$

Pošto je $0 < r_1 - r_2 < b$ i b je prost broj, $t = (r_1 - r_2)^{-1} \bmod b$ postoji i može biti izračunat u polinomijalnom vremenu od strane Ivane koristeći Euklidov algoritam. Stoga imamo da je:

$$v^{(r_1 - r_2)t} \equiv \left(\frac{y_2}{y_1}\right)^{bt} \pmod n.$$

Također

$$(r_1 - r_2)t = lb + 1$$

za neke pozitivne brojeve l, pa imamo

$$v^{lb+1} \equiv \left(\frac{y_2}{y_1}\right)^{bt} \pmod{n},$$

ili ekvivalentno tome:

$$v \equiv \left(\frac{y_2}{y_1}\right)^{bt} (v^{-1})^{lb} \pmod{n}.$$

Ako su obje strane kongruencije potenciramo s b^{-1} mod $\varphi(n)$, dobijemo sljedeće:

$$u^{-1} \equiv \left(\frac{y_2}{y_1}\right)^{t} (v^{-1})^{l} \pmod{n}.$$

Ako izračunamo inverz modulo n s obje strane kongruencije dobijemo sljedeću formulu za u:

$$u = \left(\frac{y_1}{y_2}\right)^{t} v^{l} \pmod{n}.$$

Ivana može koristiti ovu formulu da izračuna u u polinomijalnom vremenu.

Primjer 7.2. *Kao u prethodnim primjerima, pretpostavimo da je $n = 223693$, $b = 503$, $u = 101576$ i $v = 89888$. Pretpostavimo da je Ivana otkrila da je:*

$$v^{401}103386^b \equiv v^{375}93725^b \pmod{n}.$$

Prvo izračuna

$$\begin{aligned} t &= (r_1 - r_2)^{-1} \pmod{b} \\ &= (401 - 375)^{-1} \pmod{503} \\ &= 445. \end{aligned}$$

A zatim

$$\begin{aligned} l &= \frac{(r_1 - r_2)t - 1}{b} \\ &= \frac{(401 - 375)445 - 1}{503} \\ &= 23. \end{aligned}$$

U konačnici može dobiti tajnu vrijednost od u na sljedeći način:

$$\begin{aligned} u &= \left(\frac{y_1}{y_2}\right)^t v^l \pmod{n} \\ &= \left(\frac{103386}{93725}\right)^{445} 89888^{23} \pmod{223693} \\ &= 101576. \end{aligned}$$

Time je Anin tajni eksponent kompromitiran.

7.1 Identifikacijske sheme bazirane na identiteti

Guillou-Quisquater identifikacijska shema može biti transformirana u takozvanu identifikacijsku shemu baziranu na identiteti. To znači da certifikati nisu potrebni no svejedno trebamo TA, koji će izračunati vrijednost od u kao funkciju Aninog ID stringa. Računanje vrijednosti u je prikazano u Algoritmu 11.

Algoritam 11 (Izdavanje vrijednosti u Ani)

1: TA utvrdi Anin identitet i izda identifikacijski string $ID(Ana)$.
2: TA izračuna $u = (h(ID(Ana))^{-1})^a \bmod n$ i proslijedi u Ani.

U ovoj shemi h je javna hash funkcija koja poprima vrijednosti iz $\mathbb{Z}_n$ (h se može konstruirati kao odgovarajuća modifikacija od SHA-1). Vrijednost od u je RSA šifrat, koji TA računa koristeći tajni enkripcijski eksponent a gdje je $a = b^{-1} \bmod \varphi(n)$. Identitet-bazirana identifikacijska shema je opisana u Algoritmu 12.

Algoritam 12 (Guillou-Quisquater identitet-bazirana identifikacijska shema)

1: Ana odabere nasumičan broj k, gdje je $0 \leq k \leq n-1$ i izračuna $\gamma = k^b \pmod{n}$.
2: Ana da $ID(Ana)$ i γ Borisu.
3: Boris izračuna $v = h(ID(Ana))$.
4: Boris odabere nasumičan broj r, takav da je $0 \leq r \leq b-1$ i proslijedi ga Ani.
5: Ana izračuna $y = ku^r \pmod{n}$ i pošalje y Borisu.
6: Boris verificira $\gamma \equiv v^r y^b \pmod{n}$.

8 Literatura

[1] J. A. Buchmann, *Introduction to Cryptography*, Springer, 2001.

[2] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[3] J. Piepryzk, T. Hardojono, J.Seberry, *Fundamentals of Computer Security*, Springer, 2003.

[4] A. Salomaa, *Public-Key Cryptography*, Springer, 1990.

[5] Doug Stinson, *Cryptography, Theory and practice*, 3rd edition, 2005.

9 Sažetak

Identifikacija nam je potrebna zbog sprječavanja krađe identiteta kod razmjene podataka na daljinu. U radu smo naveli nekoliko različitih identifikacijskih shema kao što su Schnorrova, Okamotova i Guillou-Quisquaterova. Također opisali smo potpunost i zvučnost identifikacijske sheme što nam je bilo potrebno za dokaz idetifikacijske sheme bez znanja. Svaka identifikacijska shema ima svoju pouzdanost koja je u radu prikazana pomoću vjerojatnosti da se prevarant upješno lažno predstavi.

Ključne riječi

identifikacijske sheme, osobna autentikacija, vjerojatnost, Guillou-Quisquater, Schnorr, Okamoto, diskretni algoritam

10 Title and summary

Identification schemes and entity authentication
The identification is needed to prevent the identity theft when the data is exchanged. Several different identification schemes like Schnorr, Okamoto and Guillou-Quisquater are mentioned. Furthermore, in order to prove the zero-knowledge identification scheme, the completeness and soundness are described. Every identification scheme has its own trustworthiness. The trustworthiness is presented as the probability that the thief can misrepresent himself in the network successfully.

Key words

identification schemes, entity authentication, probability, Guillou-Quisquater, Schnorr, Okamoto, discrete algorithm

11 Životopis

Rođen sam 7. srpnja 1989. godine u Osijeku. Završio sam Osnovnu školu Višnjevac u Višnjevcu te III. gimnaziju u Osijeku. Tijekom osnovnoškoloskog obrazovanja sudjelovo sam na županijskim natjecanjima iz matematike. Nakon završenog Sveučilišnog preddiplomskog studija matematike upisao sam Sveučilišni diplomski studij matematike, smjer Matematika i računarstvo.

Od veljače 2016. do travnja 2017. radio sam u tvrtki Mono kao software developer.