UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Anja Stražar

Dokazi brez razkritja znanja

Seminar iz Kriptografije

Ljubljana; 2004

Kazalo

S pojmom kriptografija označujemo šifriranje informacij zaradi zaščite podatkov. Kriptografija se tradicionalno ukvarja z načrtovanjem in analizo "skrivne" komunikacije med dvema stranema. Dandanes pa je tesno povezana z računalništvom in komunikacijo preko interneta. Tako se ukvarja tudi z drugimi problemi, kot sta na primer konstrukcija digitalnih podpisov in identifikacija. S temi problemi pa so zelo povezani dokazi brez razkritja znanja in zato bomo tekom seminarja spoznali osnovno teorijo dokazov brez razkritja znanja in identifikacijo z njimi.

Oglejmo si dialog:

Anita: "Jaz pa poznam geslo od Pentagona in sestavine McDonald's-ove skrivnostne omake!"
Bojan: "Ne, ne veš."
Anita: "Ja pa vem."
Bojan: "Ne, ne veš!"
Anita: "Ja vem!"
Bojan: "Dokaži!"
Anita: "Naj ti bo!"in zašepeta Bojanu na uho.
Bojan: "Zanimivo! Sedaj pa jaz tudi vem in lahko povem naprej."
Anita: "O joj!"

Ali je možno dokazati neko izjavo tako, da pri tem ne razkrijemo nobene informacije o njej? Leta 1985 je Shafi Goldwasser [**10**] s sodelavci predstavila teorijo interaktivnih dokazov in *dokazov brez razkritja znanja*, ki imajo pomembno vlogo v kriptografiji.

Dokazi brez razkritja znanja omogočajo identifikacijo, izmenjavo ključev in implementacijo drugih osnovnih kriptografskih operacij brez odtekanja skrivnih informacij med pogovorom. Ker potrebujejo manjše računalniške kapacitete kot drugi javni protokoli, so zelo vabljivi pri uporabi pametnih kartic.

1 Teorija dokazov brez razkritja znanja

V matematiki je dokaz fiksno zaporedje trditev, ki so bodisi očitno pravilne bodisi izpeljane iz prejšnjih veljavnih trditev. Dokazi so tako statični. V vsakdanjem življenju pa se o nečem prepričamo tekom pogovora oziroma interakcije. Dokazi so dinamični in jih ne obravnavamo kot fiksen objekt, ampak kot proces ugotavljanja veljavnosti trditve. Dokazi brez razkritja znanja so tako interaktivni kriptografski protokol med dokazovalcem, ki dokazuje svojo trditev, in razsodnikom, ki od dokazovalca želi dokaz.

Najlaže pa razložimo dokaze brez razkritja znanja **z jamo Ali Babe** [**5**]: Jama Ali Babe je jama, ki se konča z dvema rovoma, katera se s poznavanjem skrivnega gesla na koncu skleneta. Primož pozna geslo in želi o tem prepričati Vero, ne želi pa ji razkriti samega gesla. Tako odideta do jame, kjer Primož prosi Vero, da počaka pred vhodom, medtem ko se on skrije v njej. Nato naj odide v jamo do razpotja rovov in pove, iz katerega rova naj pride; levega ali desnega. In Primož pride ven po željenem rovu.

Postopek nato ponavljata toliko časa, da je Vera prepričana, da Primož res pozna skrivno geslo. Primož bo, če pozna geslo, vsakič prišel po pravem rovu, ker bo po potrebi odprl skrivna vrata z geslom. Če pa ne pozna gesla, bo po pravem rovu prišel najverjetneje le v polovici primerov.

Poleg dokazovalca Primoža, ki ima neko informacijo in je ne želi posredovati Veri, in razsodnika Vere, ki Primožu postavlja raznorazna vprašanja, da bi se prepričala ali Primož res pozna skrivnost, pa v interaktivnih protokolih nastopajo še prisluškovalka Eva in zlobni Matic. Eva prisluškuje pogovoru med Primožem in Vero. Dober dokaz brez razkritja znanja mora preprečiti, da Eva izve karkoli o skrivnosti in da ne bo mogla nikogar drugega prepričati, da pozna skrivnost. Zloben Matic, ki prisluškuje pogovoru, pa pošilja dodatna sporočila ter spreminja in uničuje sporočila med Primožem in Vero. Dober protokol mora biti odporen tudi za taka dejanja.

Ta imena se bodo pojavljala skozi ves seminar in so postavljena tako, da se njihove začetnice ujemajo z angleškimi besedami njihovi vlog:

Primož	prover	dokazovalec
Vera	verifier	razsodnik
Eva	eavesdropper	prisluškovalec
Matic	malice	zlobnež

V kriptografiji protokol dokaz brez razkritja znanja običajno poteka tako, da dokazovalec pozna rešitev nekega težkega matematičnega problema. Na primer, faktorizacijo zelo velikega števila, ki je produkt le dveh praštevil. Nato pa ga z naključno transformacijo pretvori v izomorfen problem. Dokazovalec zna rešiti tudi ta izomorfen problem, saj pozna tako naključno transformacijo kot tudi rešitev prvotnega problema. Razsodnik nato od dokazovalca zahteva bodisi dokaz, da sta oba problema izomorfna, bodisi pa rešitev novega problema. Če dokazovalec pozna pravilno rešitev prvotnega problema, bo lahko odgovoril na obe vprašanji. Če pa ne pozna pravilne rešitve, lahko razsodnik zahteva ravno tisti odgovor, ki ga ne pozna, in tako izvedel, da dokazovalec ne pozna rešitve problema oziroma naključne transformacije.

Kriptografsko strukturo dokazov brez razkritja znanja lepo demonstrira primer **z rubikovo kocko**:
Recimo, da Primož zna rešiti rubikovo kocko in želi o tem preričati tudi Vero, ne želi pa Vere naučiti samega reševanja. Skeptična Vera da Primožu rubikovo kocko in želi, da jo reši. Primož ponujeno kocko premeša in pokaže Veri novo postavitev rubikove kocke. Vera nato prosi Primoža, da ji pokaže, kako dobimo iz tega položaja kocke tistega, ki mu ga je dala, ali pa da ji pokaže, kako se reši kocka iz tega novega položaja.

Če Primož zna rešiti rubikovo kocko, lahko odgovori na obe zahtevani vprašanji. Če pa Primož ne zna rešiti kocke, lahko odgovori le na eno od zastavljenih vprašanj. Na prvo vprašanje zna odgovoriti, če si je sproti zapisoval mešanje. Na drugo pa le, če je goljufal in vzel že rešeno kocko, ki jo je nato premešal. Poznavanje obeh odgovorov namreč pomeni poznavanje skrivnosti rubikove kocke. Zato je ključnega pomena, da Primož vsakič Veri pokaže drugo postavitev kocke, saj bi sicer Vera dobila oba odgovora in se naučila rešiti rubikovo kocko.

Tehniki protokola dokaz brez razkritja znanja pravimo deli in izberi[1], saj je podobna klasičnemu protokolu poštenega deljenja:

- Anita razdeli določeno stvar na dva dela,
- Bojan izbere eno polovico,
- Aniti ostane preostala polovica.

Ker prvi svojo polovico izbira Bojan, je za Anito najbolje, da razdeli v prvem koraku pravično, saj se ji bo po vsej verjetnosti pripetilo, da ji bo ostal manjši delež.

Tehnika deljenja in izbire pri protokolu dokaz brez razkritja znanja deluje, ker Primož ne more vedno pravilno uganiti Verine izbire. Če na primer, v primeru z jamo Ali Babe, Primož ne pozna skrivnosti, bo lahko prišel ven le po tistem rovu, po katerem je šel noter. Primož v vsakem krogu lahko ugane Verino izbiro z verjetnotjo 50%. Če mu tako Vera ne verjame po prvem krogu in postopek ponovita, lahko tudi v drugem krogu pravilno ugane z verjetnostjo 25%. Verjetnost, da pretenta Vero, se na vsakem koraku razpolovi in je tako po n krogih enaka 1 proti 2^n. Po 10 krogih je tako verjetnost, da Primož ne pozna gesla, 1 proti $2^{10} = 1024$, t.j.: $0,097\,\%$.

[1] cut and choose

1.1 Značilnosti dokazov brez razkritja znanja

Dokaz brez razkritja znanja je kriptografski protokol, ki ne razkrije informacije oziroma skrivnosti same med izvajanjem. Med protokolom razsodnik ne izve ničesar takšnega, kar ne bi mogel tudi brez dokazovalca. Ker na koncu razsodnik še vedno ne pozna skrivnosti, se ne bo mogel predstavljati kot dokazovalec nikomur drugemu. Tudi če posname pogovor z dokazovalcem, s tem posnetkom ne bo uspel nikogar prepričati, saj njegov sogovornik ne bo postavljal vprašanj v enakem vrstnem redu kot jih je on.

Protokol dokaz brez razkritja znanja pa onemogoča tudi goljufanje, tako z ene kot z druge strani. Ker se verodostojnost sleparja v nekaj krogih protokola zelo zmanjša, dokazovalec skoraj ne more ogoljufati razsodnika. Če dokazovalec ne pozna skrivnosti, bo kogarkoli prepričal le z zelo veliko sreče. Ob prvem napačnem odgovoru pa bo razkrit. Protokol deluje celo, kadar je možnost, da dokazovalec odgovor ugane več kot $\frac{1}{2}$. Potrebnih je le več krogov izvajanja.

Dokazi brez razkritja znanja so zgrajeni tako, da razsodnik ne dobi nobene informaciji, niti če se protokola ne drži. Med protokolom se informacija ne posreduje in se tako le prepriča, da dokazovalec res pozna skrivnost. Dokazovalec vedno razkrije le eno od mnogih rešitev problema. Nikoli pa vseh rešitev, saj bi sicer razsodnik lahko našel skrivnost sam.

Primer z jamo Ali Babe lepo demonstrira vse te značilnosti dokazov brez razkritja znanja. Ko Primož prepriča Vero, da resnično pozna skrivnost jame, Vera še vedno ne pozna skrivnosti. Niti, če ne upošteva Primoževih navodil in kuka, v kateri rov je odšel. Prav tako pa tudi Primož ne more pretentati Vere, ker nikoli ne ve, kateri rov bo izbrala.

1.2 Načini delovanja

Do sedaj je protokol dokaz brez razkritja znanja potekal interativno. Primož in Vera se izmenjajoče pogovarjata; en sprašuje, drugi odgovarja. Tako zaupanje zgradita postopoma v n krogih. Kaj pa, če bi izvedli vseh n krogov hkrati; vzporedno?

1. Primož problem z n naključnimi števili pretransformira v n različnih izomorfnih problemov. S poznavanjem rešitve in vseh n naključnih števil lahko Primož reši vseh n problemov.

2. Vera se za vsakega od teh n problemov odloči ali želi vedeti rešitev problema ali dokaz, da je res izomorfen prvotnemu.

3. Primož ji odgovori na vseh n vprašanj.

Ta način izvajanja protokola je primeren za slabe oziroma počasnejše povezava, saj število potrebnih interakcij zelo zmanjšamo.

Prvotno so dokaze brez razkritja znanja zgradili za potrjevanje znanja brez interakcij. Kako svetu povedati, da nekaj veš, brez da bi to dejansko povedal?

V osnovi neinterativni dokazi brez razkritja znanja delujejo enako kot vzporedni, le da Verino vlogo prevzame enosmerna zgoščevalna funkcija[2].

1. Primož problem pretransformira z n naključnimi števili v n različnih izomorfnih problemov, tako kot pri vzporednem protokolu.

2. Primož na sestavljenih problemih uporabi zgoščevalno funkcijo. Prvih n bitov njenega rezultata predstavlja odločitev ali želimo rešitev novega problema ali dokaz, da je res izomorfen prvotnemu. Če na i-tem mestu v nizu stoji 1, želimo za i-ti problem izvedeti odgovor na prvo vprašanje, sicer pa na drugo.

3. Primož odgovori na izbranih n vprašanj in objavi prvoten in izomorfne probleme, zgoščevalno funkcijo z rezultatom in vseh n izbranih rešitev.

4. Kdor se želi prepričati, da Primož res ima rešitev prvotnega problema, mora tako le preveri, če so bili vsi trije predhodni koraki pravilno izvedeni.

Primož torej lahko objavi, da poseduje neko informacijo, brez njenega razkritja in o tem prepriča vse skeptike. Če bi hotel Primož goljufati, bi moral pravilno predvideti izhodni niz zgoščevalne funkcije, ki je naključni generator bitov. Ob nepoznavanju skrivnosti namreč Primož lahko odgovori le na eno od zastavljenih vprašanj, ne pa na obe.

Protokol pa lahko uporabimo tudi za digitalne podpise. Vhodni podatki zgoščevalne funkcije so, v tem primeru, identifikacijski podatki in sporočilo, ki ga želimo podpisati.

1.3 Računska zahtevnost

Računska zahtevnost dokazov brez razkritja znanja je veliko manjša od kriptografije javnih ključev. V tujih virih največkrat zasledimo, da lahko z njimi

[2]one-way hash function

dosežemo enake rezultate kot z javnimi ključi z enim do dveh velikostnih redov $\left(\frac{1}{10}\right.$ do $\left.\frac{1}{100}\right)$ manj računske moči. Tipična implementacija dokazov brez razkritja znanja zahteva 20 do 30 modularnih množenj pri polni dolžini bitnega niza. S pravilnim preračunavanjem pa lahko to optimiziramo na 10 do 20 množenj. Torej so dokazi brez razkritja znanja veliko hitrejši od RSA.

Največja prednost uporabe dokazov brez razkritja znanja namesto javnih ključev je tako nizka računska zahtevnost. Včasih nam prav pridejo tudi določene njihove lastnosti, vendar pa bi največkrat lahko enako uspešno uporabili tudi kriptografijo javnih ključev. Odločilna prednost je torej nizka računska zahtevnost.

Mehanizem dokazov brez razkritja znanja nam dovoljuje, da protokol razdelimo na ponavljajoče se lahke operacije, namesto da izvajamo eno zahtevno operacijo, kar nam minimizira časovno in spominsko zahtevnost. Vendar pa je spominska zahtevnost približno enaka zahtevnosti javnih ključev, saj za visoko raven varnosti dokazov brez razkritja znanja, potrebujemo zelo dolge ključe in številke.

1.4 Kriptografska moč

Podobno kot tudi drugi kriptografski protokoli tudi dokazi brez razkritja znanja uporabljajo običajno kriptografsko matematiko; modulsko računanje, diskretno matematiko, teorijo velikih števil...

Kriptografska moč dokazov brez razkritja znanja temelji na reševanju težkih problemov, kot so na primer:

- računanje diskretnega logaritma velikih števil
- Ali je število kvadratno po modulu n, kjer je n veliko število, katerega faktorizacije ne poznamo?
- faktorizacija velikih števil, ki so produkt samih velikih praštevil

Varnost dokazov brez razkritja znanja temelji na istem principu kot ostali kriptosistemi. Pri njih se pojavljajo enaki problemi kot pri javnih ključih in, če bi iznašli enostaven algoritem za njihovo reševanje, bi odpovedalo zelo veliko kriptografskih sistemov. Zato moramo ob nenehno zmogljivejših računalnikih izbirati ključe primerno dolge današnjemu času. Nekaj varnosti pa lahko pridobimo tudi z časovno omejitvijo Primoževega odgovora Veri, s čimer naj bi onemogočili napad z grobo silo[3] in vmesnim napadalcem[4].

[3] brute force attack

[4] man in the middle attack

2 Identifikacija z dokazi brez razkritja znanja

V resničnem svetu svojo identiteto dokazujemo z fizičnimi dokazi; kot so osebna izkaznica, potni list, vozniško dovoljenje, kreditna kartica in zdravstvena kartica. Z dokazi, ki vsebujejo bodisi našo sliko bodisi naš podpis. V digitalnem svetu pa žal nimamo oprejemljivih dokazov o naši identiteti.

Leta 1987 so Uriel Feige, Amos Fiat in Adi Shamir predlagali identifikacijo z dokazi brez razkritja znanja; [**6**] in [**7**]. V digitalnem svetu vsakemu dodelimo identifikacijsko številko, ki je tako osnova za naš identifikacijski dokaz. Z dokazi brez razkritja znanja nato lahko vsak dokaže svojo identiteto, brez da bi razkril svojo identifikacijsko številko.

Ideja je zelo dobra, saj nam omogoča dokazovanje identitete brez fizičnih dokazov. Vendar pa ni popolna. Poglejmo si nekaj primerov zlorabe:

Problem šahovskega mojstra: Anita, ki ne zna igrati šaha, bi rada postala največji šahovski mojster. Tako povabi na turnir dva največja mojstra ob istem času na isti kraj. Mojstra posede v sosednji sobi, tako da ne vesta drug za drugega. Anita z enim igra bele figure z drugim pa črne. Ko prvi mojster naredi potezo, si jo Anita zapomni in isto potezo odigra pri drugem. Nato isto ponovi pri drugem mojstru. Igro nadaljujejo dokler nekdo ne zmaga. Oba mojstra mislita, da igrata z Anito, čeprav v resnici igrata drug proti drugemu. Anita tako premaga enega od dveh največjih mojstrov in postane veliki šahovski mojster, čeprav sama sploh ne zna igrati šaha.

Problem mafijske goljufije: Ko je Adi Shamir predstavil identifikacijo z dokazi brez razkritja znanja, je rekel, da bi lahko miljonkrat zapored lahko šel v mafijsko trgovino, pa ga še vedno ne bi mogli ogoljufati. Vendar se je zmotil! Mafija lahko ogoljufa človeka, ki v njihovi restavraciji poceni večerja in mu zaračuna nakup dragega nakita. Vse kar mora storiti je, da prestreže elektronska plačilna sporočila.

Recimo, da Anita večerja v mafijski restavraciji, medtem ko se mafijski pajdaš spehaja po dragi draguljarni. Ko po večerji Anita želi plačati in dokazati svojo identiteto mafija iz restavracije obvesti svojega pajdaša, ki se tako ob istem času odpravi plačati nakit. Ko Anita dokazuje svojo identiteto mafiji, ta posreduje navodila svojemu pajdašu, ki tako izvede enak protokol v draguljarni. Ko draguljar postavi vprašanje pajdašu, ta posreduje vprašanje mafiji, ki enako vprašanje zastavi Aniti. Nič hudega sluteča Anita odgovori na vprašanje. Mafija pa odgovor posreduje svojemu pajdašu. Namesto, da bi Anita dokazala svojo identiteto mafiji v restavraciji, jo dokaže draguljarju in kupi drag nakit.

Problem goljufije teroristov: V tem primeru Anita želi pomagati teroristu pri vstopu v državo. Ko na uradu za priseljevanje terorista sprašujejo, jim ta posreduje odgovore, ki jih dobi po radijski zvezi od Anite. Na uradu bodo tako verjeli, da se pogovarjajo z Anito in v državo spustili terorista. Tri dni kasneje pa se terorist s kombijem polnim eksploziva pripelje do neke vladne ustanove.

Obe omenjeni goljufiji sta mogoči, ker so zarotniki povezani z radijsko zvezo. Če bi torej identifikacija potekala v Faraday-evi kletki, kjer ni signala, do goljufije sploh ne bi moglo priti. Pri problemu šahovskega mojstra pa bi morali Anito prisiliti, da sedi dokler igra ni končana. Namesto tega sta Thomas Beth in Yvo Desmedt predlagala drugačno rešitev; [**8**]. Če vsak korak protokola časovno omejimo, bi zarotnikom zmanjkalo časa za komunikacijo. Na primer, če mora biti vsaka poteza pri šahovskem mojstru narejena v 1 minuti, Anita ne bi imela dovolj časa za tekanje iz sobe v sobo.

Problem večih identitet: Včasih pri dodeljevanju identifikacijskih številk ne preverijo že registriranih uporabnikov in enemu uporabniku dodelijo več identifikacijskih številk. Anita ima tako lahko več identitet in lahko stori kaznivo dejanje in izgine. Če Anita neko identiteto uporabi le enkrat, je ne bodo mogli izslediti.

Problem posojanja identitet: Anita želi odpotovati v ZDA, a ne dobi vize. Zato ji prijateljica ponudi svojo identiteto. (Prvi se je sicer ponudil Bojan, a ima žal eno napako.) Anita od prijateljice dobi identifikacijsko številko in odpotuje v Ameriko. Medtem ko je Anita v Ameriki, ima ta prijateljica popoln alibi za kriminalna dejanja zunaj ZDA. Kako naj bi storila karkoli drugod, če pa je v ZDA? Popolen alibi pa ima tudi Anita, saj bo za vsa dejanja kriva prijateljica.

Ta prevara je mogoča, ker v digitalnem svetu vedno dokazujemo le, da poznamo neko informacijo, neko zaporedje bitov. Nikoli ne dokažemo, kdo res smo.

2.1 Feige – Fiat – Shamirjeva identifikacijska shema

Feige – Fiat – Shamirjeva identifikacijska shema je najbolj znana identifikacijska shema. Spremlja pa jo prav nenavadna zgodba; [**9**]. 9 julija 1986 so trije avtorji podali prošnjo za pridobitev patenta pri ameriškem uradu za patentiranje. Zaradi možne vojaške uporabe je prošnjo pregledala tudi ameriška vojska. Včasih se tako v takih primerih zgodi, da urad namesto patenta izda ukaz o tajnosti. 6. januarja 1987, 3 dni pred iztekom polletnega roka, je tako

urad na zahtevo vojske izdal poročilo, v katerem je pisalo: "Kakeršnokoli razkrivanje ali objavljanje te vsebine škoduje nacionalni varnosti."Avtorjem so naročili, da morajo vse Američane, katerim je bila vsebina že razkrita, obvestiti, da bo vsako nedovoljeno razkrivanje vsebine kaznovano z dvemi leti zapora in 10.000$ kazni. Poleg tega pa morajo avtorji obvestiti tudi vse urade za patentiranje v državah, katerih državljani so drugi ljudje, katerim je bila vsebina že razkrita.

To pa je popolna norost, saj so avtorji predstavili svoje delo na konferencah v Izraelu, Evropi in Ameriki že pred pol leta. Poleg tega pa avtorji sploh niso bili Američani, njihove raziskave pa so bile narejene na Weizmannovem inštitutu v Izraelu. Novica se je razširila tako med akademiki kot tudi po časopisih. Po dveh dneh so ukaz preklicali, avtorji pa verjamejo, da je posredovala NSA, čeprav o tem uradno ne želijo govoriti.

Po Feigu, Fiatu in Shamirju se identifikacija začne v centru zaupanja, ki generira naključno število n kot produkt dveh velikih praštevil. Center zaupanja generira tudi Primožev javni in zasebni ključ. Javni ključ je obrnljivo število v, ki je kvadratni ostanek po modulu n; t.j.: $m^2 = v \bmod n$ za neko število m in $\exists\ v^{-1} \bmod n$. Zasebni ključ pa je najmanjše tako število s, za katero je $s = \sqrt{v^{-1}} \bmod n$. Poenostavljena verzija sheme poteka takole:

1. Primož izbere poljubno število $r < n$, izračuna $x = r^2 \bmod n$ in število x pošlje Veri.

2. Vera pošlje Viktorju naključen bit $b \in \{0, 1\}$.

3. Če Primož dobi od Vere 0, ji nazaj pošlje r, sicer pa $y = r \cdot s \bmod n$.

4. Če je bil $b = 0$, Vera preveri $x = r^2 \bmod n$, od koder sledi, da Primož pozna $\sqrt{x}$. Sicer pa preveri $x = y^2 \cdot v \bmod n$, kar pomeni, da Primož pozna $\sqrt{v^{-1}}$.

Shemo nato Primož in Vera ponavljata dokler Vera ni postopoma prepričana, da Primož res pozna svoj zasebni ključ s.

Koraki identifikacijske sheme so podobni korakom dokazov brez razkritja znanja. Zato pravimo, da je to identifikacija z dokazi brez razkritja znanja. Na koncu identifikacije Vera še vedno ne pozna Primoževega zasebnega ključa. Ve le, da Primož zagotovo pozna pravi zasebni ključ. Če bi se nekdo drug izdajal za Primoža in ne bi imel zasebnega ključa, ne bi mogel izbrati takega r, da bi lahko odgovoril Veri v obeh primerih. Na vsakem koraku izvajanja sheme je tako verjetnost, da sleparja razkrijemo 50%. Po n korakih je verjetnost, da je Primož slepar, 1 proti 2^n. Podobno pa se tudi Vera ne more

izdajati za Primoža, saj je 50% verjetnost, da njen sogovornik na vsakem koraku ne izbere enakega bita kot ga je ona.

V tem postopku je bistveno, da Primož na vsakem koraku izbere drugo število r, saj bi v nasprotnem Vera dobila oba odgovora in bi tako lahko izračunala Primožev privatni ključ.

Feige – Fiat – Shamirjevo identifikacijsko shemo lahko implementiramo tudi vzporedno. Na začetku enako kot prej generiramo naključno število n. Zasebni in javni ključ pa generiramo enako kot prej, le da moramo tokrat izbrati k različnih kvadratnih ostankov po modulu n: $v_1, v_2, ..., v_k$, ki predstvaljajo javni ključ. Zasebni ključ $s_1, s_2, ..., s_k$ pa nato izračunamo po formuli $s_i = \sqrt{v_i^{-1}}$. Identifikacija vzporedno poteka takole:

1. Primož izbere $r < n$, izračuna $x = r^2 \bmod n$ in število x pošlje Veri.
2. Vera pošlje Primožu k bitni niz $b_1 b_2 ... b_k$.
3. Primož izračuna $y = r \cdot \left(s_1^{b_1} \cdot s_2^{b_2} \cdot ... \cdot s_k^{b_k}\right) \bmod n$ in ga pošlje Veri.
4. Vera preveri, ali je $x = y^2 \cdot \left(v_1^{b_1} \cdot v_2^{b_2} \cdot ... \cdot v_k^{b_k}\right) \bmod n$.

Tokrat je po n korakih verjetnost, da je Primož slepar 1 proti 2^{kn}.

2.2 Guillou – Quisquaterjeva identifikacijska shema

Feige – Fiat – Shamir je bila prva uporabna identifikacijska shema. Narejena je tako, da računsko zahtevnost minimizira s povečanjem števila interacij. Kar pa je pri majhnih sistemih, kot je, na primer, pametna kartica, prej slabost kot prednost. Pri plačevanju s kartico namreč potrebujemo hitro identifikacijo.

Louis Guillou in Jean-Jacques Quisquater sta razvila identifikacijo z dokazom brez razkritja znanja prav v te namene. Algoritem je zasnovan tako, da je potrebna le ena interacija. Vendar pa je pri veliki stopnji varnosti njegova računska zahtevnost veliko večja od Feige – Fiat – Shamirjeve sheme.

Ker je identifikacijska shema namenjena uporabi pametnih kartic, v nadaljevanju Primoževo vlogo prevzame pametna kartica. Pametna kartica vsebuje neke identifikacijske podatke, ki so zapisani z bitnim nizom J. Na primer, na bančni kartici je zapisana njena številka, od katere banke je, veljavnost, bančni račun... Po analogiji s ključi je niz J javni ključ. Na vsaki pametni kartici pa je zapisan tudi eksponent v in modul n, s katerima je določen njen zasebni ključ B; $JB^v = 1 \bmod n$.

Pri plačevanju s kartico se prenese niz J v čitalec, kartica pa mora nato še dokazati, da so to res njeni identifikacijski podatki oz. dokazati mora, da pozna zasebni ključ B. Protokol poteka takole:

1. Kartica zgenerira naključno število r med 1 in $n-1$ in čitalcu pošlje $T = r^v \bmod n$.
2. Čitalec zgenerira naključno število d med 0 in $v-1$ in ga pošlje kartici.
3. Kartica izračuna $D = rB^d \bmod n$ in pošlje čitalcu.
4. Čitalec preveri, ali je $T = D^v J^d \bmod n$. Če je, je identifikacija potrjena.

3 Uporaba dokazov brez razkritja znanja

V tem poglavju si bomo dokaze brez razkritja znanja ogledali še s praktičnega vidika. Predstavljeni teoretični protokoli so relativno težko izračunljivi in potrebujejo dolge ključe za zadovoljivo stopnjo varnosti, kar zahteva zmogljive računalnike in velike spominske kapacitete. Pametne kartice in čipi vgrajeni v razno raznih napravah pa imajo veliko manjšo zmogljivost od namiznih računalnikov.

Poglejmo si nekaj največkrat uporabljenih kriptografskih protokolov. Protokoli se razlikujejo tako po velikosti sporočila in številu interacij kot tudi po računski in spominski zahtevnosti. Primerjavo med protokoli prikazuje tabela:

Protokol	Velikost sporočila	Število interacij	Računska zahtevnost	Spominska zahtevnost
Dokazi brez razkritja znanja	velika	veliko	velika	velika
Kriptografija javnih ključev	velika	ena	zelo velika	velika
Simetrični algoritmi	majhno	ena	majhna	majhna

Najbolj ekonomičen je simetričen algoritem; npr.: DES in AES; ki pa nam žal nudi najnižjo stopnjo varnosti in so tako za plačilne kartice ne uporabni. Poiskati moramo protokol, ki ima najustreznejše razmerje med računsko in spominsko zahtevnostjo ter varnostjo. Ne obstaja enolična izbira

protokola za vse naše potrebe. Na pametne kartice so največkrat implementirani dokazi brez razkritja znanja, saj so varnejši od simetričnih algoritmov in lažje izračunljivi od javnih ključev.

Verjetno mislite, da je plačilna kartica, zdravstvena kartica... dobro zaščitena in so podatki na njih nedostopni. Mnogo pametnih kartic je zavarovanih le do neke stopnje in še to ne vse. Obstaja mnogo primerov preveč poenostavljene uporabe kriptografije. Zaradi pomanjkanja računalniške moči in dobrih algoritmov se, na primer, kartice za satelitske sprejemnike razbijejo z najenostavnejšimi kriptografskimi tehnikami. Tako za večino satelitskih sistemov lahko dobimo že kopije piratskih kartic.

Nekaj zaščite pa bi potrebovali tudi vgrajeni čipi v različnih daljinskih upravljalcih; npr.: za zaklepanje avta, garažnih vrat, televizijski daljinec; in drugih napravah, kot sta računalniška miška in mikrovalovna pečica. Ker pa so te naprave največkrat cenovno omejene, so v njih vgrajeni najcenejši čipi, ki nimajo veliko spomina in računske zmogljivosti. V teh sistemih si ne želimo 100% varnost, temveč le zadovoljivo. V mislih moramo vedno imeti pravo razmerje med kriptografijo, viri in potrebno varnostjo.

V kriptosistemu je potrebna raven varnosti ravnotežje med očitnimi napadi in ugodnostmi, ki jih ščitijo. Sistem moramo zavarovati le toliko, da se napadalcem časovno in denarno ne izplača. Za dolgočasne in nezanimive naprave z vgrajenimi čipi je tako ta raven zelo nizka.

3.1 Implementacija dokazov brez razkritja znanja

Običajni čipi imajo med 24 in 256 bytov delovnega spomina – RAM. Nekateri imajo potem še 64 bytov trajnega spomina – EEPROM, kar bi lahko uporabili za skrivno skrivališče podatkov ali ključa. Čipi so torej veliko manj zmogljivi kot namizni računalniki in zato moramo protokol dokaz brez razkritja znanja nekoliko prilagoditi. Prilagodimo ga lahko na 3 načine:

1. pri posameznih korakih dokazov brez razkritja znanja izvajamo enostavnejše operacije, ki ne potrebujejo veliko računske moči. Če je interacijski korak enostaven, lahko večkrat ponovimo interacijo in tako povečamo našo verodostojnost.

2. protokol zahteva, da se vsak korak zaključi v minimalnem času. Če bomo uporabljali hitre sisteme, bo zahtevnost napada z grobo silo tako narasla, da se napadalcem cenovno ne bo izplačal.

3. uporabljamo protokole, na katerih ni izvedljiv hitri napad s slovarjem niti, če ima napadalec zelo velike spominske zmoglivosti.

3.2 Napadi na dokaze brez razkritja znanja

Tehnologija za branje zavarovanega spomina ali vzratni inžiniring[5] procesorjev in pomnilnikov pamentinih kartic je presenetljivo dobra in največkrat dokaj enostavna za uporabo. Posamezne tehnike delimo na:

- Enostavne tehnike, kjer z uporabo nestandardne napetosti izbrišemo zaščitno kodo.
- Specializirane tehnike, kjer z magnetom skeniramo delovanje čipa.
- Drage in vsestranske tehnike, kjer s kislino odstranjujemo plast po plast z čipa.

Poleg omenjenih napadov na pametne kartice, pa so možni tudi neposredni napadi na same dokaze brez razkritja znanja. Najbolj pogosti so:

Spominski napad: Napadalec lahko pri veliki kapaciteti spomina sestavi tabelo izomorfnih problemov in posameznih odgovorov, ki jih dobi od dokazovalca. S pomočjo tabele svoj napad nato toliko pospeši, da ga izvede v časovnih omejitvah.

Napad z grobo silo: Napadalec lahko s svojim vsemogočnim računalnikom reši problem v omejenem času. Časovne omejitve moramo postaviti tako, da je ta napad ne izvedljiv.

Post-mortem napad z grobo silo: Napadalec lahko protokol posname in ga skuša razbiti kasneje, brez časovnih, računalniških in spominskih omejitev. Ta napad je možen tudi pri drugih protokolih. Obranimo pa se ga lahko s spreminjajočim se geslom. Na primer, če vemo, da se ključ lahko odkrije v nekaj dneh z zelo močnim računalnikom, protokol postavimo tako, da se ključ spremeni vsak dan. Napadalec bo tako po nekaj dnevih dobil ključ, ki ni več v uporabi.

Post-mortem napad z grobo silo je resna krožnja vsem šibkejšim in oslabljenim kriptosistemom. Če ključa oz. skrivnosti ne spreminjamo dovolj pogosto, lahko kdorkoli izvede napad z grobo silo na posnetku pogovora. Še posebno pri minimalističnih rešitvah, ko je dolžina ključa minimalna zaradi hardwarskih omejitev, je to lahko resen problem.

Ob pravilnem razmerju varnostnih potreb in sistemskih zmožnosti še vedno lahko postavimo zadovoljivo zanesljiv sistem, namesto ne zavarovanih sedanjih. Implementacija resnično zavarovanega sistema zahteva velike računske

[5] reverse engineer

in spominske zmožnosti. Pri aplikacijah, kjer je zahtevana stopnja varnosti visoka, moramo tako uporabiti zmogljivejše čipe, na katerih lahko deluje polnomočni kriptografski protokol. Druga rešitev pa je, da uporabimo simetrične kriptografske protokole, ki imajo nizke računske in spominske zahteve.

Združevanje dobrih kriptografskih tehnik in protokolov z omejitvami majhnih sistemov je zelo težko. Večina študij kriptografije je namreč osnovanih na dovolj močnih računalnikih in zadostni kapaciteti spomina.

Literatura

[**1**] B. SCHNEIER: Applied Cryptography, *John Wiley & Sons, Inc (1996)*, 101 – 111 in 503 – 510

[**2**] H. A. ARSONSSON: Zero Knowledge Protokols and Small Systems; http://www.tml.hut.fi /Opinnot/Tik-110.501/1995/zeroknowledge.html

[**3**] O. GOLDREICH: Zero Knowledge: a tutorial by Oded Goldreich; http://www.wisdom.weizmann.ac.il/∼oded/zk-tut02.html

[**4**] RSA security: What are interactive proofs and zero-knowledge proofs?; http://www.rsasecurity.com/rsalabs/node.asp?id=2178

[**5**] J. J. QUISQUATER, L. GUILLOU, T. BERSEN: How to Explain Zero Knowledge Protocols to Your Children; http://www.dice.ucl.ac.be/crypto/publications/1990/alibaba.pdf

[**6**] A. FIAT in A. SHAMIR: How to Prove Yourself: Practical Solutions to Identification and Signature Problems, *Advances in Cryptology - CRYPTO '86 Proceedings*, 186 – 194

[**7**] A. FIAT in A. SHAMIR: Unforgeable Proofs od Identity, *Proceedings of Securicom '87*, 147 – 153

[**8**] T. BETH in Y. DESMEDT: Identification Tokens–or: Solving the Chess Grandmaster Problem, *Advances in Cryptology - CRYPTO '90 Proceedings*, 169 –176

[**9**] S. LANDAU: Zero Knowledge and the Department of Defense; *Notice of the American Mathematical Society;* jan. 1988, 5 –12

[**10**] S. GOLDWASSER, S. MICALI in C. RACKOFF: The Knowledge Complexity of Interactive Proof - Systems; *Proceeding of STOC '85;* maj 1985, 291 –304