Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.9
DOI: https://doi.org/10.24867/31BE31Poznanovic

DOKAZI NULTOG ZNANJA

ZERO KNOWLEDGE PROOFS

Isidora Poznanović, *Fakultet tehničkih nauka, Novi Sad*

Oblast – RAČUNARSTVO I AUTOMATIKA

Kratak sadržaj – *U ovom radu je predstavljen koncept dokaza nultog znanja, njihov kriptografski značaj i primene. Prikazana je osnovna podela na interaktivne i neinteraktivne dokaze nultog znanja. Prikazana su i upoređena tri neinteraktivna protokola nultog znanja: ZK-SNARK, ZK-STARK i Bulletproofs. Predstavljen je problem kvadratnog ostatka koji je dokazan pomoću oba tipa dokaza nultog znanja. Neinteraktivni protokol koji je korišćen za dokazivanje problema kvadratnog ostatka je ZK-SNARK. Dokaz je realizovan u programskom jeziku Python, uz pomoć python-snark biblioteke.*

Ključne reči: *Dokaz nultog znanja, ZK-SNARK, ZK-STARK, Kriptografija*

Abstract – *This paper presents zero knowledge proofs, their cryptographic significance and applications. It presents a basic classification: interactive and non-interactive zero knowledge proofs. It presents and compares three protocols of non-interactive zero knowledge proofs: ZK-SNARK, ZK-STARK and Bulletproofs. It presents the quadratic residue problem and proofs it with both interactive and non-interactive zero knowledge proofs. The non-interactive protocol used to prove the quadratic residue problem is ZK-SNARK. The proof is implemented in the Python programming language, using python-snark library.*

Keywords: *Zero knowledge proof, ZK-SNARK, ZK-STARK, Cryptography*

1. UVOD

Pojam dokaza je opšte poznat i široko korišćen u raznim oblastima različitih nauka. Najtipičniji primer dokaza je matematički dokaz. Matematički dokaz se u osnovi sastoji iz fiksnog broja koraka pomoću kojih se iz opšte prihvaćenih činjenica (aksioma) dolazi do tvrdnje koja je dokazivana. Dokazi nultog znanja imaju isti cilj kao i matematički dokazi, da validiraju ispravnost neke tvrdnje, međutim način na koji to rade je drugačiji.

Inicijalno, dokazi nultog znanja su bili interaktivni, pa su bili sličniji dokazima u zakonu ili debati nego matematičkim dokazima, jer se istinitost tvrdnje u ovakvim dokazima verifikuje dinamičkom interakcijom više strana.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Aleksandar Kupusinac, red. prof.

Interakcija može biti skupa i spora, pa su uloženi napori da se ona vremenom izbaci iz dokaza nultog znanja, koji na taj način postaju neinteraktivni. Neinteraktivni dokazi mogu se porediti sa dokazima iz matematike ili formalne logike. Analogno dokazima u naučnim radovima, neinteraktivni dokazi nultog znanja trebaju biti univerzalni i sadržati sve potrebne informacije za validaciju bez ikakve dodatne interakcije. Ali za razliku od dokaza u naučnim radovima, neinteraktivni dokazi nultog znanju ne smeju otkrivati nikakve dodatne informacije osim činjenice da je dokazivana tvrdnja tačna.

2. DEFINICIJA DOKAZA NULTOG ZNANJA

Dokazi nultog znanja su se prvi put pojavili 1985. godine, u radu *The knowledge complexity of interactive proof systems* koji su objavili *Shafi Goldwasser*, *Silvio Micali* i *Charles Rackoff*. U tom radu je data definicija dokaza nultog znanja koja se i danas koristi [1]:

Protokol nultog znanja je metod kojim jedna strana (dokazivač) može dokazati drugoj strani (verifikatoru) da je određena tvrdnja tačna, bez otkrivanja bilo kakvih informacija osim činjenice da je određena tvrdnja tačna.

Navedeni rad daje matematičke osnove ovog metoda i navodi prve primere dokaza nultog znanja. Dokazi nultog znanja su se od tada konstantno unapređivali, pronašli su upotrebu u realnosti i danas su široko korišćeni. Zahvaljujući ovom radu postavljena je osnova za mnoge kriptografske protokole koji se i danas koriste.

U nastavku je dat primer u kome se mogu koristiti dokazi nultog znanja kao i benefiti njihovog korišćenja:

Postoji tvrdnja *"Ja imam više od 18 godina"* koju korisnik želi da dokaže nekom servisu. Kako bi korisnik to dokazao potrebno je da dostavi važeći identifikacioni dokument, poput lične karte ili pasoša, koji sadrži njegovu godinu rođenja. Dostavljanjem ličnog dokumenta servisu korisnik se izlaže riziku, rizikuje svoju privatnost. Najveća opasnost koja vreba korisnika je krađa identiteta. Ona se najčešće dešava usled hakerskih napada kada servisi skladište podatke u centralizovanim bazama podataka.

U ovakvim situacijama bolje je koristiti dokaze nultog znanja koji nisu podložni rizicima standardnog pristupa. Protokol nultog znanja koristi, kao ulaz, početnu tvrdnju na osnovu koje generiše sažet dokaz njene istinitosti. Dokaz pruža garanciju da je tvrdnja istinita bez upotrebe informacije koja je korišćena da se on napravi. Stoga kako bi korisnik dokazao servisu da ima više od 18 godina potrebno je da priloži dokaz nultog znanja. Servis treba da proveri da su odgovarajuća svojstva dokaza tačna i znaće

da je dokazivana tvrdnja tačna. U nastavku će biti razmatrano koja su to svojstva, kakvi sve nulti dokazi postoje i kako funkcionišu.

Slika 1. *Vizuelni opis dokaza nultog znanja [2]*

3. ELEMENTI DOKAZA NULTOG ZNANJA

U dokazima nultog znanja učestvuju dve strane: dokazivač i verifikator. Ukoliko se dokazivač ili verifikator pridržavaju protokola nultog znanja korektno, kažemo da su pošteni. Svaki dokaz nultog znanja neke tvrdnje mora zadovoljavati sledeća tri svojstva:

1. **Kompletnost** - ukoliko je tvrdnja tačna, protokol sa nultim znanjem uvek vraća *tačno*. Bilo koji pošteni dokazivač će ubediti bilo kog poštenog verifikatora u istinitost tvrdnje.
2. **Ispravnost** - ukoliko je tvrdnja netačna, teorijski je nemoguće prevariti protokol nultog znanja da vrati *tačno*. Ni jedan lažljivi dokazivač ne može prevariti ni jednog poštenog verifikatora da poveruje da je netačna tvrdnja tačna (postoji izuzetak zanemarivo male verovatnoće).
3. **Nulto znanje** - verifikator ne može naučiti ništa o tvrdnji osim njene istinitosti.

4. TIPOVI DOKAZA NULTOG ZNANJA

Dokazi nultog znanja mogu biti interaktivni ili neinteraktivni. Interaktivni dokazi uključuju uzajamnu komunikaciju između dokazivača i verifikatora, dok neinteraktivni dozvoljavaju dokazivaču da generiše jedan dokaz koji će verifikator kasnije koristiti nezavisno od dokazivača.

4.1. Interaktivni dokazi nultog znanja

U svojoj osnovnoj formi dokazi nultog znanja su interaktivni i sastoje se iz tri elementa: svedoka, izazova i odgovora.

- Svedok - Dokazivač želi da dokaže znanje o nekoj skrivenoj informaciji verifikatoru. Ta skrivena informacija je *svedok* dokaza. Dokazivač na osnovu znanja o svedoku pravi grupu pitanja na koje može odgovoriti samo strana koja ima znanje o skrivenoj informaciji. Dakle, dokazivač započinje proces dokazivanja tako što nasumično bira pitanje, računa odgovor i šalje ga verifikatoru.
- Izazov - Verifikator nasumično bira drugo pitanje i pita dokazivača da mu odgovori.
- Odgovor - Dokazivač prihvata pitanje, računa odgovor i vraća ga verifikatoru. Na osnovu odgovora dokazivača, verifikator može otkriti da li on ima skrivenu informaciju. Da bi se osigurao da dokazivač ne nagađa odgovore, verifikator može slati više pitanja. Pitanja šalje sve dok ne bude smatrao da je verovatnoća da dokazivač slučajno pogađa tačne odgovore dovoljno mala.

4.2. Neinteraktivni dokazi nultog znanja

Iako su interaktivni dokazi nultog znanja bili značajno otkriće, potreba za konstantnom povezanošću i interakcijom između dve strane je značajno ograničavala njihovu primenu. Čak i kada bi verifikator bio ubeđen u znanje dokazivača dokaz bi bio nedostupan nekom drugom verifikatoru koji želi da proveri istu informaciju. Kako bi se ovaj problem rešio predstavljeni su neinteraktivni dokazi nultog znanja u kojima verifikator i dokazivač imaju deljeni ključ [3].

Za razliku od interaktivnih dokaza, neinteraktivni zahtevaju jednokratnu komunikaciju između verifikatora i dokazivača. Dokazivač prosleđuje tajnu informaciju specijalnom algoritmu koji računa dokaz nultog znanja. Dokaz se šalje verifikatoru koji proverava da li dokazivač zna tajnu informaciju koristeći drugi algoritam. Jednom kada je dokaz izgenerisan on je dostupan i drugim verifikatorima koji imaju pristup deljenom ključu i verifikacionom algoritmu. Pritom verifikator nije u stanju da rekonstruiše originalnu informaciju iz dokaza.

Ovaj tip dokaza je posebno koristan u slučaju da je komunikacija između strana ograničena ili skupa. Neinteraktivni dokazi nultog znanja imaju dosta podtipova koji su prevashodno razvijeni za različite potrebe primene.

4.2.1. ZK-SNARK

ZK-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) je protokol nultog znanja koji pravi sažeti dokaz koji može biti proveren brzo i ne iziskuje interaktivnu komunikaciju dokazivača i verifikatora [4].

Ovim protokolom su zadovoljena ranije pominjana svojstva kompletnosti, ispravnosti i nultog znanja. Sažetost dokaza generisanih uz pomoć ZK-SNARK protokola se ogleda u maloj veličini dokaza i efikasnoj verifikaciji.

Veličina generisanih dokaza je konstantna ili raste logaritamski u odnosu na veličinu aritmetičkog kola kojim se ispituje tačnost zadate tvrdnje. Pa je veličina dokaza kompleksnih problema gotovo jednaka veličini dokaza jednostavnih problema i obično iznosi par stotina bajtova.

Verifikacija dokaza je kratka i izvršava se u mnogo kraćem vremenskom periodu nego računanja u aritmetičkom kolu [5].

4.2.2. ZK-STARK

ZK-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge) je protokol predstavljen u radu [6] iz 2018 godine. Protokol je sličan prethodno objašnjenom protokolu, najbitnije razlike se ogledaju u pojmovima skalabilnosti i transparentnosti.

Skalabilnost je jedna od ključnih osobina ovog protokola, ona omogućava način da se kreira sažet i efikasan dokaz za širok spektar proračuna. Pa je ovaj protokol pogodan za različite aplikacije uključujući blokčejn i decentralizovane sisteme. ZK-STARK je dosta brži u generisanju i verifikovanju dokaza kako veličina svedoka raste, sa povećanjem svedoka blago se linearno povećavaju vremena da se izgeneriše i verifikuje dokaz.

ZK-STARK je dizajniran da bude transparentan. Njegova sigurnost se ne oslanja na nedokazane pretpostavke i kompleksne matematičke strukture. Nasumičnost koja se koristi za generisanje parametara za dokazivanje i verifikaciju je javno dostupna te nema potrebe za pouzdanom ceremonijom postavljanja ključeva.

4.2.3. Bulletproofs

Bulletproofs protokol je prvi put predstavljen u radu [7] iz 2018. godine kao protokol sa neprobojnim sigurnosnim pretpostavkama, kratak kao metak. Dizajniran je tako da u određenim scenarijima bude skalabilniji i efikasniji od ZK-SNARK protokola. Najbolje se primenjuje u dokazima opsega, gde dokazivač želi da pokaže da se tajna vrednost nalazi unutar nekog opsega bez otkrivanja ostalih informacija o tajnoj vrednosti. Ovaj protokol nultog znanja generiše kratke dokaze logaritamske veličine u odnosu na veličinu svedoka i nije mu potrebna pouzdana ceremonija postavke ključeva. Bulletproofs protokol se kao i ZK-SNARK oslanja na kriptografiju eliptičnih kriva, čija sigurnost koja je zasnovana na tome da je izuzetno teško izračunati diskretni logaritam u eliptičkim krivama. Za klasične računare, diskretni logaritamski problem na eliptičkim krivama je eksponencijalno težak ali je u kvantnim računarima ovaj problem rešiv u polinomijalnom vremenu.

Ovaj protokol je usvojen od strane raznih kriptovaluta poput Monera. Pri prelasku na Bulletproofs zapaženo je smanjenje od 80% u veličinama transakcija.

4.2.4. Poređenje neinteraktivnih protokola

U nastavku je prikazan odnos prethodno opisanih neinteraktivnih protokola. Najveća mana i slaba tačka ZK-SNARK protokola nalazi se u ceremoniji postavljanja ključeva. U protokolu ZK-STARK te ceremonije nema, jer on koristi transparentne heš protokole sa polinomkim IOP [8]. Bulletproofs protokol koristi argumente unutrašnjeg proizvoda zasnovane na eliptičkim krivama kojima nije potrebno pouzdano podešavanje ključeva.

ZK-SNARK ima konstantnu veličinu dokaza, dokazi su kratki i ne zavise od kompleksnosti problema. Nešto veći dokazi kreiraju se kroz Bulletproofs protokol, oni rastu logaritamski sa porastom kompleksnosti, dok ZK-STARK generiše najveće dokaze koji su polilogaritamski. Ali, bez obzira što su dokazi ovog protokola najduži, oni se generišu u kvazilinearnom vremenu pa se time i najbrže generišu, jer ostala dva protokola iziskuju linearno vreme. Kada je u pitanju vreme verifikacije dokaza, najmanje vremena je potrebno ZK-SNARK protokolu, a najviše Bulletproofs protokolu [9].

5. KRIPTOGRAFSKI ZNAČAJ

Matematika kriptografije je inicirana primenama u stvarnom svetu. Najosnovnija i prvobitna primena ogleda se u želji da se privatno komunicira u prisustvu prisluškivača koji osluškuje komunikaciju. Sa pojavom računara kao sredstva za komunikaciju, pojavljuju se brojne druge primene, od verifikacije autentičnosti podataka i pristupnih privilegija do omogućavanja složenih finansijskih transakcija preko interneta koje uključuju više strana, od kojih svaka ima svoje poverljive informacije.

5.1. Upotreba dokaza nultog znanja u kriptografiji

Goldreich, *Micali* i *Wigderson* su u radu *How to Prove All NP Statements in Zero-Knowledge* 1987. godine dokazali da se za svaki problem iz *NP* klase problema može konstruisati dokaz nultog znanja. Ova činjenica nameće dokaze nultog znanja kao veoma moćan alat u modernoj kriptografiji. Veza kriptografije i dokaza nultog znanja nalazi se u konceptu zaštite poverljivih informacija i osiguravanja bezbednosti podataka. Kriptografija omogućava alate za zaštitu informacija, dok dokazi nultog znanja pružaju sigurnu proveru tih informacija bez otkrivanja poverljivih podataka. Dokazi nultog znanja koriste se kao metoda za očuvanje sigurnosti i poverljivosti u teorijskim osnovama kriptografije, u zadacima poput generatora pseudo-nasumičnih brojeva i enkripcije. Na primer, dokazi nultog znanja omogućavaju dokazivanje autentičnosti podataka bez otkrivanja samih podataka u složenim finansijskim transakcijama u koje je uključeno više strana sa svojim sopstvenim poverljivim informacijama [10,11].

Dokazi nultog znanja su uveli jedinstven pristup u oblasti kriptografije i izdvojili su se od drugih kriptografskih protokola koji su usmereni na privatnost u distribuiranim sistemima. U master radu upoređeni su sa kriptografskim metodama homomorfnog šifrovanja i sigurnih višestranih proračuna (eng. *Secure Multiparty Computation*). Svi ovi metodi za svrhu imaju verifikaciju informacija i očuvanje privatnosti [12]. Homomorfno šifrovanje omogućava izvođenje proračuna nad šifrovanim podacima bez potrebe za dešifrovanjem [13]. Dok sigurnosni višestrani proračuni omogućavaju nepoverljivu saradnju više strana koje zajedno računaju zadatu funkciju preko njihovih ulaza koji ostaju privatni [14].

5.1. Zcash

Zcash je jedna od najznačajnih primena ZK-SNARK protokola zato što on ujedno predstavlja i prvu široko korišćenu primenu dokaza nultog znanja u praksi. Dokazima nultog znanja osigurava zaštićene transakcije u kojima pošiljalac, primalac i količina resursa prenetih transakcijom ostaju privatni [15,16].

Zcash je kriptovaluta koja je fokusirana na privatnosti i anonimnosti transakcija. Ugrubo nastao je tako što je grupa naučnika na Bitkoinov otvoreni kod dodala dokaze nultog znanja [17]. Motivacija za tim je nedostatak privatnosti Bitkoina gde su transakcije verifikovane i snimljene na javnom blokčejnu, pa svako može pristupiti korisničkim balansima i podacima o transakcijama.

Ova kriptovaluta implementira Decentralized Anonymous Payment (DAP) šemu pod nazivom Zerocash koja je detaljno opisana u radu iz 2014. godine [18]. Razlika između DAP šeme i standardnog Bitkoin sistema jeste u tome što Bitkoin sistem koristi transparentne transakcije, dok DAP šema omogućava korisnicima da vrše zaštićene transakcije (shielded transakcije). Ove transakcije skrivaju osetljive informacije, tj. skrivaju informacije o pošiljaocu i primaocu, kao i iznos transakcije. Međutim Zcash pored zaštićenih transakcija omogućava i transparentne transakcije slične onima koje Bitkoin koristi. Stoga korisnici mogu sami izabrati nivo privatnosti koji je njima potreban [19].

Provera validnosti transakcija bez otkrivanja podataka o transakciji omogućena je korišćenjem ZK-SNARK protokola. Pomoću ovog protokola učesnici u transakciji mogu da dokažu da imaju informacije koje su potrebne za izvršenje transakcije (na primer privatne ključeve), bez otkrivanja tih informacija trećoj strani. Zaštićene transakcije mogu biti u potpunosti enkriptovane u blokčejnu, ali se i dalje mogu verifikovati kao validne pod uslovima konsenzusa koristeći ZK-SNARK protokol [20].

6. ZAKLJUČAK

Dokazi nultog znanja predstavljaju revolucionarno otkriće u oblasti kriptografije, obezbeđujući sredstvo za dokazivanje znanja bez otkrivanja samog znanja. U ovom radu navedena je prva definicija ovog koncepta i osnovna podela na interaktivne i neinteraktivne dokaze nultog znanja. Upoređena su tri najpoznatija neinteraktivna dokaza nultog znanja: ZK-SNARK, ZK-STARK i Bulletproofs.

Kako tehnologija nastavlja da se razvija, primena dokaza nultog znanja se sve više širi. Dokazi nultog znanja su danas jedan od najpopularnijih metoda za osiguravanje anonimnosti transakcija pa igraju ključnu ulogu u razvoju bezbednih digitalnih sistema koji čuvaju privatnost korisnika.

7. LITERATURA

[1] Shafi Goldwasser, Silvio Micali, Sharles Rackof, "*The knowladge complexity of interactive proof systems*", Society for Industrial and Applied Mathematics, 1985.

[2] https://schor.medium.com/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1 (pristupljeno u oktobru 2024.)

DOI: https://doi.org/10.24867/31BE31Poznanovic

[4] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, Madars Virza, *"Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture"*, 23rd USENIX Security Symposium (USENIX Security 14). San Diego, CA: USENIX Association, Avg. 2014., str. 781-796. ISBN: 978-1-931971-15-7. Dostupno na: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/ben-sasson (pristupljeno u oktobru 2024.)

[5] Nir Bitansky, Ran Canetti, Alessandro Chiesa, Eran Trome, *"Recursive Composition and Bootstrapping for SNARKs and Proof-Carrying Data"*, 2012.

[6] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, Michael Riabzev, *" Scalable, transparent, and post-quantum secure computational integrity"*, 2018.

[7] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, Greg Maxwell, *"Bulletproofs: Short Proofs for Confidential Transactions and More"*, 2017.

[8] Szepieniec Alan, Zhang Yuncong, *"Polynomial IOPs for Linear Algebra Relations"*, Springer International Publishing, 2022., str. 523–552. ISBN: 978-3-030-97121-2.

[9] El-Hajj Mohammed, Oude Roelink Bjorn, *"Evaluating the Efficiency of zk-SNARK, zk-STARK, and Bulletproof in Real-World Scenarios: A Benchmark Study"*, 2024. Dostupno na: https://www.mdpi.com/2078-2489/15/8/463 (pristupljeno u oktobru 2024.)

[10] Shafi Goldwasser, *" Mathematical foundations of modern cryptography: computational complexity perspective"*, 2002. arXiv: cs / 0212055 (cs.CR). Dostupno na: https://arxiv.org/abs/cs/0212055 (pristupljeno u oktobru 2024.)

[11] Goldreich Oded, Micali Silvio, Wigderson Avi., *"How to Prove all NP Statements in Zero-Knowledge, and a Methodology of Cryptographic Protocol Design"*, sv. 263 1986., str. 171-185.

[12] Ryan Lavin, Xuekai Liu, Hardhik Mohanty, Logan Norman, Giovanni Zaarour, Bhaskar Krishnamachari "*A Survey on the Applications of Zero-Knowledge Proofs*", 2024. arXiv: 2408.00243 (cs.CR). Dostupno na: https://arxiv.org/abs/2408.00243 (pristupljeno u oktobru 2024.)

[13] Ronald L. Rivest and Michael L. Dertouzos, *"On data banks and privacy homomorphisms"*, 1978. Dostupno na: https://api.semanticscholar.org/CorpusID:6905087 (pristupljeno u oktobru 2024.)

[14] Yao, Andrew C., *"Protocols for secure computations"*, 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982). 1982., str. 160-164.

[15] What are zero-knowledge proofs, Dostupno na: https://z.cash/learn/what-are-zero-knowledge-proofs/ (pristupljeno u oktobru 2024.)

DOI: https://doi.org/10.24867/31BE31Poznanovic

[17] How is Zcash different than Bitcoin, Dostupno na: : https://z.cash/learn/how-is-zcash-different-than-bitcoin/ (pristupljeno u oktobru 2024.)

DOI: https://doi.org/10.24867/31BE31Poznanovic

[19] Sean Bowe, Daira Hopwood, Taylor Hornby, Nathan Wilcox, *"Zcash Protocol Specification"*, 2020.

[20] What are ZK-SNARKS, Dostupno na: https://z.cash/learn/what-are-zk-snarks/ (pristupljeno u oktobru 2024.)

Kratka biografija:

Isidora Poznanović rođena je u Kragujevcu 2000. god. Master rad na Fakultetu tehničkih nauka iz oblasti Elektrotehničko i računarsko inženjerstvo – računarstvo i automatika, odbranila je 2024.god.

Kontakt: isidora@uns.ac.rs