ZERO KNOWLEDGE PROOFS

1. Zero Knowledge proofs i illustrativni primeri

Nulti dokazi znanja (Zero Knowledge proofs) su vrsta kriptografskog protokola koji omogućava jednoj strani (proveravaču) da se uveri u tačnost tvrdnje koju iznosi druga strana (dokazivač), pri čemu pritom proveravač ne saznaje ništa više osim same tačnosti tvrdnje. Ovo je korisno u situacijama gde je potrebno dokazati određenu informaciju, ali se istovremeno želi zadržati privatnost.
Na primer, zamislimo da želite dokazati nekome da znate lozinku bez otkrivanja same lozinke. Možete koristiti zero knowledge proof tako što ćete odgovarati na niz pitanja koja zahtevaju znanje lozinke, ali tako da sami ne otkrijete lozinku. Na primer, osoba može tražiti da unesete karakter na određenom mestu u lozinci ili da izvršite određenu operaciju nad lozinkom. Na taj način, osoba koja proveravaće vaše znanje o lozinci, ali neće znati samu lozinku.
Ovo je samo jedan jednostavan primer, ali zero knowledge proofs su široko primenljivi u raznim oblastima, uključujući kriptovalute, digitalni identitet, i druge oblasti gde se zahteva dokazivanje bez otkrivanja poverljivih informacija.

2.Primene ZKP-a

Nulti dokazi znanja (Zero Knowledge Proofs, ZKP) imaju različite primene u kriptografiji i informacionoj bezbednosti. Evo nekoliko primera primena:
*Kriptovalute: U kriptovalutama poput Bitcoina, ZKP se koriste kako bi se omogućilo potvrđivanje transakcija bez otkrivanja identiteta učesnika ili iznosa transakcije.
*Digitalni identitet: ZKP se mogu koristiti za dokazivanje određenih atributa digitalnog identiteta, poput godina ili državljanstva, bez otkrivanja svih detalja identiteta.
*Sigurno skladištenje podataka: ZKP se može koristiti za proveru integriteta podataka bez otkrivanja samih podataka. Na primer, možete dokazati da imate određeni dokument bez otkrivanja sadržaja dokumenta.
*Autentifikacija: ZKP se mogu koristiti za dokazivanje autentičnosti bez otkrivanja tajnih ključeva ili lozinki. Na primer, možete dokazati da posedujete određen kreditnu karticu bez otkrivanja broja kartice.
*Pravo glasa: ZKP se mogu koristiti u elektronskim izbornim sistemima kako bi se omogućila provera glasa bez otkrivanja identiteta birača ili detalja njihovog glasa.
*Masinsko ucenje - prikriva deo ulaza ili ceo ulaz, za obradu osetljivih podataka

3.Merkle tree i ZK dokaz pripadnosti skupu

Merkle stablo (Merkle tree) je kriptografska struktura podataka koja se često koristi u distribuiranim sistemima, kao što su blockchain mreže, radi efikasnog provere integriteta podataka.
Osnovna ideja Merkle stabla je da se veliki skup podataka organizuje u hijerarhijsku strukturu stabla. Na vrhu stabla se nalazi jedinstveni hash (digest) koji predstavlja celokupan skup

podataka. Svaki čvor stabla, osim listova, je hash od svoje dece. Listovi stabla sadrže stvarne podatke ili hash-ove tih podataka.

Zero knowledge proof (ZKP) pripadnosti skupu se može koristiti sa Merkle stablom na sledeći način:

1. **Dokaz pripadnosti**: Da bi se dokazalo da određeni podatak pripada skupu podataka koji se čuva u Merkle stablu, korisnik može pružiti dokaz koji se sastoji od niza hash-eva koji čine put od korena stabla do određenog lista koji sadrži podatak koji želi da dokaže. Korisnik takođe može pružiti dokaz da su ti hash-ovi izračunati na osnovu validnih podataka. Na taj način, korisnik može dokazati pripadnost skupu podataka bez otkrivanja samih podataka.
2. **Efikasnost**: Korišćenje Merkle stabla omogućava efikasan dokaz pripadnosti, jer korisnik može pružiti samo logaritamski broj hash-eva u odnosu na veličinu skupa podataka. Ovo čini ZKP pripadnosti skupu korisnim u situacijama gde je potrebno efikasno dokazivanje pripadnosti velikom skupu podataka.

Ova kombinacija Merkle stabla i ZKP pripadnosti skupu često se koristi u blockchain mrežama radi efikasne provere integriteta transakcija i dokazivanja vlasništva nad određenim podacima.

4. Completeness, soundness and ZK

Kada pričamo o Nultim Dokazima Znanja (ZKPs), postoje tri važna koncepta koje treba razmotriti: potpunost, ispravnost i svojstvo nultog znanja.
1.*Potpunos*t: Ovo znači da ako je tvrdnja istinita, iskren proverilac će biti uveren u njen istinit sadržaj. Dakle, ako osoba zaista ima potrebno znanje i ispravno sledi postupak, proverilac bi trebalo da prihvati dokaz kao istinit.
2.*Ispravnost*: Ovo se odnosi na to da, ako tvrdnja nije istinita, proverilac neće biti prevaren lažnim dokazom. To znači da ni u kom slučaju proverilac neće prihvatiti lažnu tvrdnju kao istinitu.
3.*Svojstvo nultog znanja*: Ovo znači da se tvrdnja može dokazati bez otkrivanja bilo kakvih dodatnih informacija osim same tačnosti tvrdnje. Drugim rečima, proverilac neće saznati ništa više od toga da je tvrdnja zaista istinita, što garantuje privatnost i diskreciju.
Ovi koncepti su ključni za razumevanje i analizu ZKP sistema, osiguravajući da funkcionišu na pouzdan način i omogućavajući verifikaciju bez otkrivanja suvišnih informacija.

5.Ciklicna grupa

Ciklična grupa (Zp,*) je grupa obratnih elemenata u skupu cijelih brojeva modulo p, gdje je p prost broj. Ova grupa se sastoji od svih brojeva iz skupa \(\{1, 2, 3, ..., p-1\} \) koji su međusobno prosti s \(p \), a operacija je množenje modulo \(p \).
Ova grupa je ciklična jer se može generisati jednim elementom, koji se naziva generatorom grupe. Generacija se vrši tako što se počne sa nekim elementom, a zatim se taj element množi sam sa sobom modulo p, dok se ne dođe do svih elemenata grupe.
Ova grupa je od velike važnosti u teoriji brojeva i kriptografiji, posebno u algoritmima kao što su Diffie-Hellman ključna razmjena i ElGamal kriptosistem.

6.Problem diskretnog logaritma

Neka je G grupa npr Fq i neka su a,g \<in> G. Najmanji prirodan broj n (ako postoji) takav da je a = g^n zovemo diskretni logaritam od a
u osnovi g i oznacavamo sa logg(a).

7. Eliptičke krive nad konačnim poljem

U matematici, konačno polje je polje koje sadrži konačan broj elemenata. Red konačnog polja je broj njegovih elemenata, koji je ili prost broj ili prost stepen.
Eliptične krive su grupe koje su definisane nad konačnim poljima. Jednačina eliptične krive je
E: y^2 = x^3 + a*x+b
gde su a i b iz algebarskog zatvorenja konačnog polja K. Ova jednačina se naziva kratka Vejverasova jednačina za eliptične krive.
O - Tačka u beskonačnosti
Ovo znači da se skup tačaka na eliptičnoj krivi uvek ponaša kao Abelova grupa, što znači da zadovoljava sledeće osobine:
1.Zatvorenost: Ako tačke P i Q pripadaju E(K), onda i njihova suma P + Q takođe pripada E(K).
2.Asocijativnost: (P + Q) + R = P + (Q + R).
3.Identitet: Postoji identitetni element 0 takav da je P + 0 = P.
4.Inverz: Svaki element P ima inverzni element Q takav da je P + Q = 0.
5.Komutativnost: P + Q = Q + P.
Eliptična kriva nad konačnim poljem se, dakle, smatra cikličnom i zadovoljava sve navedene osobine Abelove grupe.

8. Add and Double algorithm

Kako možemo pomnožiti tačku P sa skalarnom vrednošću m gde je m≥0?
mP = P + P + P + P + … + P (m puta)
Ali taj metod je previše spor za velike m!
Za brže računanje, predstavljamo m kao binarni broj i dobijamo rezultat u logaritamskom vremenu.
Na primer, da bismo evaluirali 79*P, konvertujemo 79 u njegov binarni oblik.
Tako možemo evaluirati zbir:
$79*P = 2^6*P + 2^3*P + 2^2*P + 2^1*P + 2^0*P$

9. Multi-Scalar-Multiplication (bucket metod)

U algoritmima dokazivanja većine sistema za dokaze nultog znanja baziranih na eliptičkim krivama, usko grlo je algoritam za višestruko množenje skalara (MSM). Naivni algoritam koristi strategiju dvostrukog dodavanja. Najbrži pristup je varijanta Pipenžerovog algoritma koju nazivamo bucket metod(metod kanti)

Algoritam višestrukog množenja skalara (MSM) ključan je u procesu generisanja SNARK (succinct non-interactive arguments of knowledge) dokaza zasnovanih na eliptičkim krivama. Ovaj algoritam se koristi za efikasno množenje tačaka na eliptičkoj krivi sa odgovarajućim skalarnim vrednostima.
Naivni pristup ovom problemu, poznat kao dvostruko-dodaj algoritam, efikasan je za male instance, ali postaje neefikasan sa povećanjem broja skalarnih vrednosti. Ovo je zbog toga što zahteva veliki broj operacija dodavanja i dupliranja, što dovodi do sporosti kada se radi sa velikim brojem tačaka i skalarnih vrednosti.
Varijante Pipenžerovog algoritma, poput metode kanti, predstavljaju unapređenje nad naivnim pristupom. Ove metode se oslanjaju na podelu skalarnih vrednosti u odgovarajuće "kante" ili grupe, što omogućava efikasnije izračunavanje množenja skalara. Korišćenje ovih optimizovanih algoritama značajno ubrzava proces generisanja SNARK dokaza, čime se omogućava praktična primena sistema za dokazivanje znanja zasnovanih na eliptičkim krivama.

10.Problem diskretnog logaritma nad EK

Problem diskretnog logaritma nad eliptičkim krivama je osnovni problem u kriptografiji koji se koristi u postupcima kao što su Diffie-Hellman razmjena ključeva i digitalni potpisi. Definicija ovog problema ide ovako:
Data je eliptička kriva E nad poljem Fp , gde je p prost broj, i neka tačka P na toj krivoj. Problem diskretnog logaritma nad eliptičkim krivama sastoji se u pronalaženju celog broja k između 1 i p − 1 takvog da je kP jednak nekoj drugoj zadatoj tački Q
na istoj krivoj. Matematički rečeno, problem je pronaći k kada je kP = Q za poznate P i Q.Ovaj problem je težak za rešavanje u opštem slučaju, posebno kada je red tačke P veliki prost broj, što ga čini ključnim alatom u sigurnosti kriptografskih sistema zasnovanih na eliptičkim krivama.

11. Uparivanje na eliptičkim krivama

Za preslikavanje e : E (Fq) × E (Fq) −→ Fq \ {0} kazemo da je
uparivanje (bilinearno preslikavae) na E (Fq) ako vai
(∀P1, P2, Q ∈ E (Fq)) e (P1 ⊕ P2, Q) = e (P1, Q) · e (P2, Q)
(∀P, Q1, Q2 ∈ E (Fq)) e (P, Q1 ⊕ Q2) = e (P, Q1) · e (P, Q2)
Kazemo da je uparivanjee e dopustivo ako je
1)Nedegenerisano:
▸ (∀Q) e(P, Q) = 1 ⇒ P = O
▸ (∀P) e(P, Q) = 1 ⇒ Q = O
2)Efektivno izracunjivo

12. SNARK & STARK

SNARK je kriptografski sistem dokaza koji omogućuje jednoj strani da dokaže drugoj strani da je određena izjava tačna, bez otkrivanja dodatnih informacija osim validnosti same izjave.
Na jednostavniji način, to je način da dokažete da znate nešto (kao rešenje matematičkog problema ili lozinku) bez otkrivanja šta je to nešto.

Izraz "sucintno" se odnosi na činjenicu da je dokaz kratak, što znači da je mnogo manji u veličini u poređenju sa stvari koja se dokazuje. "Neinteraktivno" znači da se dokaz može generisati bez potrebe za komunikacijom između dokazivača i proveravača.

STARK (Scalable Transparent ARgument of Knowledge) - ne zahteva trusted setup.Prednost STARK-a je u tome što omogućava visok stepen sigurnosti i transparentnosti, dok istovremeno čuva privatnost i poverljivost podataka. To čini STARK privlačnim rešenjem u oblastima gde je neophodno obezbediti verifikaciju podataka bez izlaganja poverljivih informacija.
Ukratko, STARK predstavlja moćan alat za verifikaciju dokaza bez otkrivanja poverljivih informacija, što ga čini korisnim u različitim oblastima, uključujući finansije, blockchain tehnologije, i sigurno deljenje podataka.

13. Aritmetizacija i sistem ograničenja (system constraints) kod ZKP-a

Aritmetizacija i sistem ograničenja (ZKP) su ključni koncepti u kriptografiji, posebno u kontekstu zero-knowledge proof (ZKP), odnosno dokazivanja nultog znanja. Evo kako ovi pojmovi funkcionišu zajedno:

Aritmetizacija: Ovaj proces se odnosi na pretvaranje problema u matematičke izraze ili operacije. U kontekstu ZKP-a, aritmetizacija se koristi za pretvaranje nekog problema ili tvrdnje u matematički izraz koji se može proveriti ili osporiti.

Sistem ograničenja: Ovaj deo je ključan za konstrukciju ZKP-a. Sistem ograničenja je skup matematičkih izraza ili ograničenja koji opisuju validne rešenja problema ili tvrdnje. Ova ograničenja se koriste za generisanje dokaza koji demonstriraju da neko rešenje ili tvrdnja zadovoljavaju tačno ova ograničenja.

Kada se ovi koncepti primene zajedno u ZKP-u, dobijamo metod za dokazivanje da posedujemo određenu informaciju ili znanje, a da ne otkrivamo samu informaciju. Na primer, ako želimo da dokažemo da posedujemo određenu tajnu vrednost x, možemo aritmetizovati problem tako da se svodi na proveru matematičkih izraza koji uključuju x, ali ne otkrivaju samu vrednost x. Zatim, koristimo sistem ograničenja da generišemo dokaz koji demonstrira da poštujemo ta ograničenja, ali ne otkriva vrednost x.

Ovi koncepti su ključni za mnoge primene u kriptografiji, kao što su autentifikacija bez izlaganja podataka, anonimno glasanje i privatno deljenje informacija. ZKP pruža moćne alate za očuvanje privatnosti i sigurnosti u digitalnom svetu.

14. Komitmenti pomoću polinoma (Polynomial Commitments) kod SNARK-ova

Komitmenti pomoću polinoma (Polynomial Commitments) su ključni element u kriptografskim konstrukcijama kao što su SNARK-ovi (succinct non-interactive arguments of knowledge). Polinomijalni komitment omogućuje dokazivanje da korisnik

posjeduje određeni polinomijal, ali bez otkrivanja samog polinoma. Ideja je da se polinomijal komprimira u jedinstvenu vrijednost (kao komitment), koja može biti javno dostupna, ali nije moguće saznati iz nje sam polinomijal.

U kontekstu SNARK-ova, ovi komitmenti se koriste za dokazivanje ispravnosti izračunavanja bez otkrivanja samih podataka ili računskih koraka. Koristeći polinomijalne komitmente, možete "zaključati" izračun ili podatke, a zatim generirati dokaz da su ti podaci ispravno obrađeni ili da ispunjavaju određene uvjete, bez otkrivanja tih podataka ili detalja izračunavanja.

Ovaj pristup omogućuje da se računski intenzivni zadaci obavljaju na decentraliziranim sustavima, kao što su blockchain mreže, bez potrebe za otkrivanjem osjetljivih podataka ili koraka izračunavanja. To je ključni element za postizanje privatnosti, sigurnosti i skalabilnosti u ovim sustavima.

15. Trusted setups kod Groth16 i PLONK-a

Trusted setup je ključan koncept u kriptografiji koji se koristi u mnogim protokolima zasnovanim na nultom znanju dokaza poput zk-SNARKS (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge). Groth16 i PLONK su dva popularna protokola koji koriste zk-SNARKS.

U Groth16 protokolu, potreban je jednokratni "trusting setup" proces koji generiše parametre za proveru ispravnosti. Ovaj proces uključuje generisanje ključeva koji se koriste za kreiranje i verifikaciju zk-SNARKS dokaza. Međutim, ukoliko se ovaj proces ne izvrši na odgovarajući način, to može dovesti do mogućnosti manipulacije od strane napadača.

PLONK (Plonk je akronim za "Permutation arguments for Linear, Observable, Noninteractive Knowledge") je noviji protokol koji je dizajniran da minimizuje rizik povezan sa setup procesom. On koristi tehnike kao što su "universal" parametri koji se mogu koristiti za više primena, što smanjuje potrebu za ponovnim sprovođenjem setup procesa za svaku pojedinačnu primenu. Ovo smanjuje potencijalne sigurnosne probleme i olakšava proces implementacije.

U oba slučaja, ključno je da setup proces bude transparentan i da učesnici imaju poverenja u njegovu ispravnost. Postoje različiti pristupi za povećanje transparentnosti i poverenja, uključujući multi-party computation (MPC) i javno svedočenje (public witnessing). Ovi pristupi omogućavaju učesnicima da zajedno sprovedu setup proces, što povećava poverenje u integritet generisanih parametara.

16. Non-Interactive Preprocessing argument system

Non-Interactive Preprocessing (NIP) argument system je vrsta sistema za proveru ispravnosti koji omogućava proveru dokaza bez interakcije sa proveravačem. Ovaj sistem je posebno koristan u kontekstu nultog znanja dokaza poput zk-SNARKS (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), gde se koriste kratki dokazi koji mogu biti provereni bez potrebe za interakcijom sa onima koji su ih generisali.

NIP argument sistemi koriste preprocesiranje ili "preprocessing" fazu gde se generišu određeni parametri ili podaci koji se kasnije koriste za verifikaciju dokaza. Ova faza se obično izvršava jednokratno i ne zahteva prisustvo korisnika tokom provere dokaza. Nakon što su parametri generisani, korisnici mogu koristiti ove parametre za brzu verifikaciju velikog broja dokaza.

Ovaj pristup je posebno koristan u aplikacijama gde je potrebno brzo i efikasno proveriti veliki broj dokaza, kao što su kriptovalute, blockchain tehnologija, privatnost podataka i mnoge druge. NIP argument sistemi omogućavaju efikasnu verifikaciju dokaza bez potrebe za skupim interakcijama ili dugotrajnim izračunavanjima.

17. KZG - KZG (trusted setup) - Kate Zaverucha Goldberg 2010
KZG je kriptografska šema koja se koristi pri komitovanju preko polinoma.
Omogućava dokazivanje ispravnosti polinoma, bez otkrivanja polinoma.
Generiše se komit za polinom i šalje se verifikatoru koji proverava da li je vrednost polinoma u određenoj tački zaista 0.

Faze KZG:

- **setup** – odaberemo nasumičnu tačku i parametre $H_0 = G$, $H_1 = Gs$, $H_2 = Gs^2$ …
- **commit** - com(f) = f(s) * G, gde s pripada konačnom polju F_p, a G je generator
- **evaluate** – $f(x_0) = y$, gde je x_0 nula $f(x) - y$ i $x - x_0 \mid f(x) - y$
  $f(s) - f(z) = (s - z) * h(s)$

Group $\mathbb{G}=\{0, G, 2G, 3G, \ldots, (p-1)G\}$ of order p.
➔ Setup($\boldsymbol{\lambda}$) —> pp:
- Sample random s from $\boldsymbol{F}$;
- pp=(H0=G, H1=s*G, H2=s*s*G, …, Hd= s*...*s*G);
- Delete s.

➔ Commit (pp, f) —> com_f where com_f:=f(s)*G

f(x)=f0+f1x+...+fdx*...*x => com_f=f0*H_0+ f1*H1+...+fd*Hd=f0*G+f1*s*G+...+fd*s*...*s*G
=(f0+f1*s+...+fd*s*...*s)*G=f(s)*G

Schwartz - Zippel lemma
For $0 \neq f \in \boldsymbol{F}^{(\leq d)}[x]$ and random $r \in \boldsymbol{F}$ than $Pr[f(r)=0] \leq d/p$.
Suppose $p \approx 2^{256}$ and $d \leq 2^{40}$ then d/p is negligible.
For different $f,g \in \boldsymbol{F}^{(\leq d)}[x]$ and random $r \in \boldsymbol{F}$ than $Pr[f(r)=g(r)] \leq d/p$.
So if f(r)-g(r)=0 w.h.p. f(x)=g(x).

Eval (Prover P, Verifier V):
f(x0)=y ⇔ x0 is a root of f-y ⇔ (x-x0) divides f-y ⇔ exist q such that q(x)*(x-x0) = f(x)-y

Prover	**Verifier**
Compute q(x)	accept if
Compute com_q —---------->	(s -x0)*com_q=com_f-y*G
	((s-x0)*q(s))*G= (s-x0)*q(s)*G=(f(s)-y)*G

18. PLONK

PLONK je vrsta protokola nultog znanja koji se koristi u kriptografiji i blockchain tehnologiji. Ovaj protokol omogućava dokazivanje tačnosti tvrdnji o zadovoljavanju aritmetičkih kola (arithmetic circuits) bez otkrivanja samih podataka ili kola.

PLONK je dizajniran da bude efikasan u poređenju s drugim ZKP protokolima. To uključuje bržu proveru dokaza i manje zahtevne resurse za generisanje i proveru dokaza.

Parametrizacija je važna karakteristika PLONK-a. To znači da se protokol može prilagoditi različitim tipovima aritmetičkih kola, što ga čini fleksibilnim za različite primene. Protokol se mora pažljivo dizajnirati kako bi se osiguralo da se tačnost dokaza može proveriti bez mogućnosti da se lažni dokazi prođu kao validni.

U suštini, PLONK u ZKP predstavlja moćan alat za postizanje privatnosti, sigurnosti i efikasnosti u različitim oblastima gde je važno dokazivanje tačnosti bez otkrivanja suvišnih informacija.

19.Protokol Semafor

Semafor je protokol sa nula znanja koji omogucava davanje signala(npr. Glasanje) bez okrivanje identiteta. Pruza jednostavan mehanizam za sprecavanje dvostruke signalizacije. Slucajevi upotrebe: privatno glasanje, otkrivanje nepravilnosti, anonimni DAO I mikseri. Semafori omogućavaju korisnicima da kreiraju objekat semafora i da ga dodaju u grupu kako bi poslali proverljiv anonimni signal.

Pomocu semafora, moguce je dozvoliti korisnicima sledece:
1. Kreiranje semafor identiteta
2. Dodavanje semafor identiteta grupi(Merkle drvo)
3. Poslati anoniman signal(npr. Glasanje)

Kada korisnik emituje signal(npr. Glasanje) semaforski dokazi bez znanja mogu osigurati da se korisnik pridruzio grupi I

Semaforsko kolo je kljucni deo protokola(srce, jezgro) I sastoji se od 3 delova:
- proof of membership – dokaz pripadnosti
- nullifier hash – anulirajuci hes
- signal – signal

Kolo hešira anulirajući heš kako bi generisao identitet komita preko koga proverava dokaz pripadnosti u korenu Merkle drveta.

Semaphore - membership proof
Kolo
Private inputs:
● treeSiblings[nLevels]: vrednosti duz Merkle putanje do obaveze identiteta korisnika
● treePathIndices[nLevels]: smer (0/1) po nivou drveta koji odgovara Merkle putanji
● identityNullifier: the 32-byte identity secret koji se koristi kao ponistavac
● identityTrapdoor: the 32-byte identity secret koji se korisi kao trapdoor

Public outputs:

- root: The Merkle koren drveta