Kvantni novac

Jelena Vujasin 51/20 RN

***Apstrakt***— Sistem za izdavanje i verifikaciju kvantnih novčanica predstavlja inovativno rešenje u domenu kvantne kriptografije. Ovaj rad detaljno opisuje proces izdavanja novčanica, strukturu kvantnih novčanica, mehanizme njihove verifikacije, kao i simulaciju pokušaja falsifikovanja. Razvijen je korisnički interfejs koji omogućava praktičnu upotrebu sistema.

Ključne reči: kvantne novčanice, kvantna kriptografija, izdavanje novčanica, verifikacija novčanica, falsifikacija.

# I. UVOD

Kvantni svet postavlja nove izazove i mogućnosti pred tradicionalne finansijske sisteme, a jedno od ključnih područja koje se ističe u ovoj transformaciji jeste koncept kvantnog novca. Dok se tehnologija razvija i ulazi u novu eru kvantnog računarstva, javlja se i potreba za istraživanjem uticaja ovih promena na finansijske tokove i monetarne sisteme. Kvantni novac, zasnovan na principima kvantne mehanike, obećava revolucionarne promene u načinu na koji obavljamo transakcije, čuvamo vrednost i razmišljamo o novcu.

# II. PREGLED LITERATURE

[1]Kriptografija je široko usvojena širom kibernetičkog prostora. Najbrži klasični računari današnjice nisu u mogućnosti da probiju osnovne matematičke sheme kriptografije, čime se osigurava poverljivost i integritet podataka svih korisnika. Međutim, predviđa se da bi budući kvantni računari teorijski mogli probiti trenutne kriptografske sisteme za samo nekoliko sati. Trenutni trenutak kada postoji dovoljno moćan kvantni računar (nazvan Y2Q) implicira da će kriptografski sistemi postati neupotrebljivi, a digitalne usluge više neće biti sigurne. To bi moglo imati katastrofalne posledice za kritične digitalne infrastrukture društva, poput onih koje pružaju holandske banke. Ovaj problem je vrlo relevantan za banke zbog obilja osetljivih podataka i informacionih tokova u sektoru koji se oslanjaju na kriptografiju, kao i zbog njihove ključne uloge u funkcionisanju društva (olakšavanje plaćanja).

[2] Infrastrukture evropskih platnih sistema kao što su T2, T2 Securities i TIPS oslanjaju se na napredne kriptografske sisteme za značajan deo svoje bezbednosti. U bliskoj budućnosti, napredak u kvantnim tehnologijama i algoritmima može učiniti današnje sigurnosne sisteme ranjivim. Međutim, kvantne tehnologije mogu takođe biti korišćene za osmišljavanje kriptografskih šema koje mogu postići bezuslovnu sigurnost i stoga su otporne na napade od strane protivnika sa neograničenim procesorskim kapacitetima. Generisanje nizova slučajnih brojeva i protokoli za sigurnu razmenu kriptografskih ključeva između dve strane osnov su svakog kriptografskog sistema. U ovom radu, koji uzima evropske platne sisteme kao referencu, analiziramo neka od rešenja trenutno dostupna za infrastrukture kvantnog generisanja slučajnih brojeva (QRNG) i distribuciju kvantnih ključeva (QKD). Da bi platni sistemi postali otporni na kvantne napade, takođe je potrebno razvijati aplikacije koje omogućavaju brzu i jednostavnu zamenu potencijalno ugroženih kriptografskih algoritama.

[3] Kodiranje konjugata je kriptografski alat koji je predstavio Stephen Wiesner krajem 1960-ih godina. To je deo dva pristupa koje je Wiesner opisao za kvantno kodiranje, zajedno sa metodom za stvaranje bankarskih novčanica koje su otporne na prevaru. Osnova koncepta je bila metoda prenosa više poruka na način da čitanje jedne poruke uništava ostale. Ovo se naziva kvantno multiplexiranje i koristi fotone polarizovane u konjugatnim osnovama kao "qubite" za prenos informacija. Kodiranje konjugata takođe predstavlja jednostavno proširenje generatora slučajnih brojeva.

[4] Princip neizvesnosti nameće ograničenja kapacitetu određenih vrsta komunikacionih kanala. Ovaj rad će pokazati da, kao kompenzaciju za ovu "kvantnu buku", kvantna mehanika omogućava nove oblike kodiranja koji nemaju analogije u komunikacionim kanalima adekvatno opisanim klasičnom fizikom.

Najpre ćemo dati dva konkretna primera kodiranja konjugata, a zatim preći na apstraktnije razmatranje.

# III. METODOLOGIJA

Ovaj projekat se sadrži iz četiri klase:Emitent, Korisnik, Enkriptor i Falsifikator. U nastavku ćemo proći logiku svake klase.

1. **Emitent:** Ova klasa, predstavlja simulaciju entiteta koji izdaje kvantne novčanice. Ključna funkcionalnost klase obuhvata generisanje i čuvanje kvantnih informacija o novčanicama, kao i proveru i verifikaciju njihovih stanja.

**Generisanje random bitova:** Generiše niz slučajnih bitova koristeći kvantno kolo sa dva qubita u superpoziciji. Simulacija se vrši pomoću simulatora Aer qasm\_simulator.

**Kreiraj novčanicu:** Kreira kvantno stanje novčanice sa zadatim brojem qubita. Svaki qubit dobija slučajno kvantno stanje, pri čemu se koristi prethodno definisana funkcija za generisanje slučajnih bitova.

**Kreiranje kvantnog serijskog broja:**

Generiše četvorocifreni serijski broj pomoću kvantnog kola sa 14 bita. Broj se dobija merenjem kvantnog stanja i konvertovanjem rezultata u decimalni broj.

**Izdaj novčanicu:** Izdaje novčanicu sa određenim brojem qubita, generiše kvantno stanje novčanice i dodeljuje joj serijski broj. Informacije o izdatoj novčanici se čuvaju u tekstualnoj datoteci, a zatim se vrši enkripcija kvantnog stanja novčanice.

**Verifikuj novčanicu:** Verifikuje novčanicu na osnovu njenog serijskog broja i kvantnog stanja. Pregleda tekstualnu bazu podataka da pronađe odgovarajući unos, dekriptuje kvantno stanje i upoređuje ga sa zadatim kvantnim stanjem radi verifikacije.

1. **Korisnik:** Klasa `Korisnik` predstavlja simulaciju entiteta koji koristi kvantne novčanice.

**Zahtevaj novčanicu:**Korisnik zahteva izdavanje nove kvantne novčanice od emitenta sa određenim brojem qubita.Informacije o novčanici se dodaju u novčanik korisnika.

**Prikaži novčanik:** Prikazuje sadržaj novčanika korisnika, odnosno sve kvantne novčanice koje je korisnik do sada dobio.

**Plati novčanicom:** Simulira proces plaćanja pomoću kvantne novčanice sa određenim serijskim brojem. Proverava validnost novčanice pozivajući funkciju za verifikaciju emitenta. Ako je novčanica validna, uklanja je iz novčanika korisnika i štampa poruku o uspešnom plaćanju. U suprotnom, štampa poruku o neuspešnom plaćanju.

Ove funkcionalnosti omogućavaju korisniku da zahteva izdavanje novih kvantnih novčanica, pregleda trenutni sadržaj svog novčanika i vrši plaćanje koristeći kvantne novčanice.

1. **Enkriptor:** Klasa `Encryptor` predstavlja simulaciju entiteta koji vrši enkripciju i dekripciju kvantnih stanja.

**Inicijalizacija:** Konstruktor klase postavlja ključ za enkripciju, gde su kvantna stanja (npr. `|0⟩`, `|+⟩`) mapirana na odgovarajuće simbole.

**Enkripcija:**Vrši enkripciju kvantnih stanja na osnovu unetog ključa. Svako kvantno stanje se zamenjuje odgovarajućim simbolom prema ključu za enkripciju.

**Dekripcija:**Vrši dekripciju enkriptovanih kvantnih stanja. Enkriptovani simboli se zamenjuju odgovarajućim kvantnim stanjima koristeći ključ za dekripciju.

Ove funkcionalnosti omogućavaju enkripciju i dekripciju kvantnih stanja, što je važno kako bi se obezbedila sigurnost i privatnost.

1. **Falsifikator:** Klasa `Falsifikator` predstavlja simulaciju entiteta koji pokušava da generiše lažne kvantne novčanice i verifikuje njihovu validnost. Evo opisa funkcionalnosti ove klase:

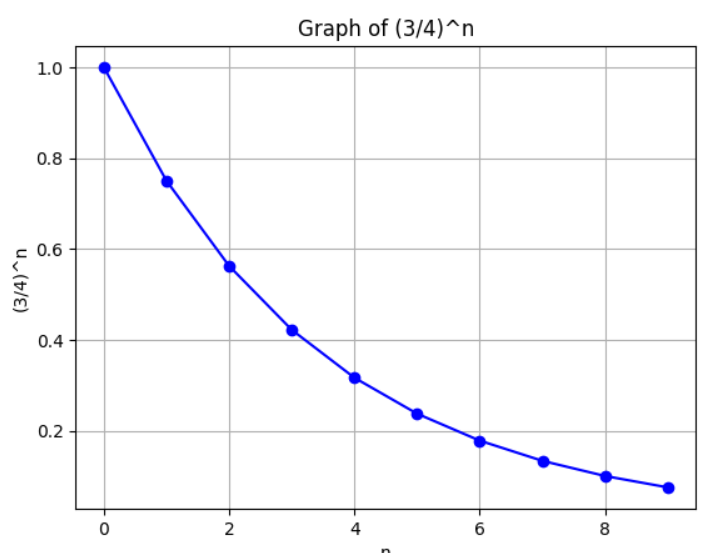
**Generiši lažnu novčanicu:** Generiše lažno kvantno stanje novčanice sa zadatim serijskim brojem i brojem qubita. Prvo se koristi emitent za kreiranje lažnog kvantnog stanja, zatim se primenjuje enkripcija na to stanje i na kraju se vraća lažna novčanica sa serijskim brojem i enkriptovanim kvantnim stanjem.

**Verifikuj lažnu novčanicu:**Vrši verifikaciju lažne novčanice pomoću emitenta. Poziva funkciju emitenta za verifikaciju, prosleđujući serijski broj i enkriptovano kvantno stanje lažne novčanice.

Ova klasa simulira proces pokušaja falsifikovanja kvantnih novčanica, gde se generiše lažno kvantno stanje i zatim pokušava verifikovati. Važno je napomenuti da ovaj kod služi isključivo u edukativne svrhe i ne predstavlja stvarne sigurnosne mehanizme.

# ANALIZA I REZULTATI

Kroz rezultate testiranja i njihovu analizu jasno se vidi da se uspešnost falsifikovanja novčanice smanjuje sa povećanjem broja kubita u novčanici.



Kao poboljšanje trebala bi se uvesti neka bolja enkripcija zbog bezbednosti stanja kubita i falsifikovanja novčanica.

# ZAKLJUČAK

Ovim projektom se pokazuje da je implementacija kvantnog računarstva u bankarstvu moguća, i da sa razvojem kvantne memorije, hardvera i softvera postoji realna mogučnost implementacije kvantnih novčanica.Rezultati ukazuju na veliki potencijal kvantnih novčanica u pružanju bezbednijih i efikasnijih metoda transakcionog poslovanja.

U narednim istraživanjima preporučuje se istraživanje novih kvantnih algoritama, poboljšanje tehnika enkripcije.

# BIBLIOGRAFIJA

1. Onkenhout Job, Secure Payments in the Quantum Era: A technology Roadmap for the Post-Quantum Cryptography Transition in the Dutch Banking Sector, 2023
2. Pietro Tiberi, Elena Bucciol, Quantum safe payment systems, 2023
3. Wikipedia, Conjugate coding, 2021
4. S.Wiesner, “Conjugate coding”, 1983