Kvantni novac

Semestarski projekat iz kvantnog računarstva

Apstrakt — Kvantni novac je kvantno kriptografski protokol za kreiranje i verifikaciju virtualne novčanice. Projekat „Kvantni novac" ima za cilj implementaciju osnovnih funkcija kvantnog bankarskog sistema u svrhu kreiranja, izdavanja i provere kvantnih novčanica kao i analizu bezbednosti kvantnog novca.

Ključne reči — Kvantni novac.

I. Opis projekta

Godine 1968. Stiven Vizner, student postdiplomskih studija na Kolumbija Univerzitetu, u svom istraživačkom radu iznosi predlog o prenosu podataka korišćenjem polarizovanih fotona i ideju o kvantnom novcu [1]. Daleko ispred svog vremena Viznerov rad "Conjugate coding"[1] nailazi na nerazumevanje i odbijanje. Rad se prvi put objavljuje tek 1983, 15 godina kasnije ali još uvek skoro 3 decenije pre pojave kvantnih računara. U godinama koje slede, zahvaljujući Viznerovim idejama razvija se kvantna teorija informacija, kvantni kriptografski metodi i kvantni komunikacioni protokoli.

Na osnovu Viznerove ideje o kvantnom kodiranju informacija, predložena je implementacija kvantnog novca prikazana na slici 1.

Izdavanje novčanice

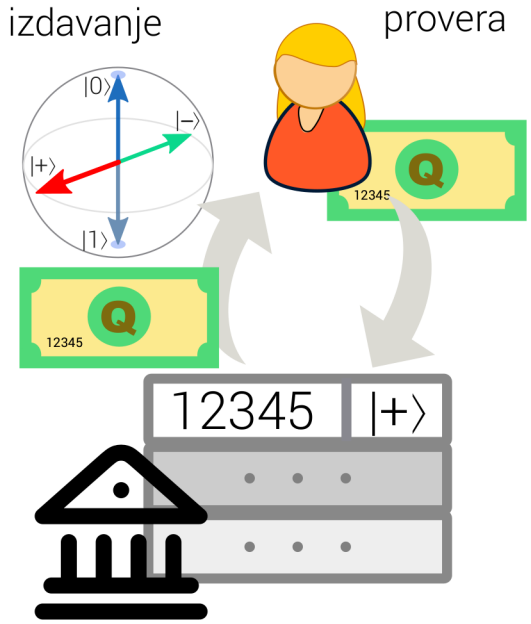
Na zahtev korisnika, kvantne novčanice izdaje emitent, npr. centralna banka, u obliku uređenog digitalno/kvantnog para $Q_n = (s, q)$, gde je:

- s jedinstveni četvorocifreni serijski broj u klasičnoj, digitalnoj formi,
- q je kubit u kvantnom stanju koje je poznato banci, ali ne i korisnicima novčanice. Kvantno stanje kubita banka bira po slučajnom izboru, npr. iz skupa $\{|0\rangle, |1\rangle, |+\rangle|-\rangle\}$.

Za svaku izdatu kvantnu novčanicu emitent u svojoj bazi podataka (glavnoj knjizi), u pogodnoj formi čuva par (s, q).

Verifikacija novčanice

Pre prihvatanja novčanice kao sredstva plaćanja, vrši se njena verifikacija slanjem (s, q) para banci. Banka u glavnoj knjizi proverava validnost novčanice i obaveštava korisnika o rezultatu.



Slika 1 . Idejni predlog implementacije kvantnog novca.

Pokušaj falsifikovanja

Teorema kvantne mehanike o zabrani kopiranja navodi da je nemoguće savršeno duplirati nepoznato kvantno stanje. To znači da falsifikator ne može kreirati lažnu kvantnu novčanicu a da ne zna kvantno stanje prave novčanice. Ipak, falsifikator može na osnovu poznatog serijskog broja generisati slučajni kubit i uspešno ga verifikovati sa verovatnoćom od 75%. U cilju sprečavanja ove vrste falsifikata i u cilju poboljšanja sigurnosti koriste se kvantne novčanice sa više kubita. Za n kubita verovatnoća pogađanja kvantnih stanja iznosi $(3/4)^n$.

[1] Termin Conjugate coding Vizner koristi u kontekstu konjugovanog para fotona koji imaju istu energiju ali suprotnu polarizaciju.

ZADATAK

Razviti osnovne komponente sistema za kvantno bankarstvo. Konkretni ciljevi projekta su:

1. Napisati program na Pajton/Qiskit programskom jeziku koji će sadržati sledeće komponente:
    1) **EMITENT**: Implementirati klasu emitenta sa potrebnim članovima za:
    (a) kreiranje,
    (b) izdavanje,
    (c) verifikaciju i
    (d) čuvanje podataka o izdatim novčanicama.
    Sistem za kreiranje novčanice treba da je fleksibilan što se broj kubita tiče. Na primer, u svrhu testiranja, mogu se izdati novčanice sa jednim kubitom, dok se u „komercijalne" svrhe izdaju novčanice sa 8 ili više kubita.
    Napisati i koristiti kvantni generator slučajnih brojeva.
    S obzirom na nepostojanje kvantne memorije, podatke čuvati u digitalnom obliku u bazi podataka, npr. SQLlite ili u tekstualnoj datoteci.
    2) **KORISNIK**: Implementirati klasu sa potrebnim članovima za:
    (a) izdavanje zahteva i prijem novčanica,
    (c) izdavanje zahteva za verifikacijom novčanica.
    3) **FALSIFIKATOR**: Implementirati klasu sa bar jednim metodom napada na kvantne novčanice.
2. Napisati jednostavni korisnički interfejs koji će omogućiti testiranje funkcija sistema: izdavanje novčanica, pregled sadržaja baze podataka sa izdatim novčanicama, verifikaciju novčanice i pokušaje falsifikovanja.

ZAVRŠNI IZVEŠTAJ I USMENA PREZENTACIJA

Završni izveštaj koji se šalje asistentu treba da sadrži tri dela:

1. Programski kod sa kratkim uputstvom za upotrebu.
2. Pisani izveštaj u zahtevanom formatu koji se može preuzeti sa RAF-ovog sajta „materijali".
3. PowerPoint prezentacija u PDF formatu.

Usmena prezentacija projekta je uz PowerPoint slajdove u trajanju od 5 minuta.

BIBLIOGRAFIJA

[1] S. Wiesner, "Conjugate coding," *ACM SIGACT News,* vol. 15, no. 1, pp. 78-88, 1983.