Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 4.4
DOI: https://doi.org/10.24867/31BE11Vukovic

INTERAKTIVNI GRAFIČKI EDITOR ZA EVALUACIJU GARBLED CIRCUITS PROTOKOLA

INTERACTIVE GRAPHICAL EDITOR FOR GARBLED CIRCUITS PROTOCOLS EVALUATION

Zorica Vuković, *Fakultet tehničkih nauka, Novi Sad*

Oblast – SOFTVERSKO INŽENJERSTVO

Kratak sadržaj – *U ovom radu je predstavljena oblast bezbednog izračunavanja sa više učesnika, kao i Yao's Garbled Circuits protokol koji predstavlja njenu osnovnu implementaciju. Opisani su sigurani načini razmene privatnih podataka pomoću Oblivious Transfer protokola. Predstavljeni protokoli su evaluirani kroz interaktivni grafički editor za evaluaciju logičkih kola koji usvaja prethodne koncepte.*

Ključne reči: *MPC, 2PC, Yao's GC protokol, logička kola, interaktivni grafički editor*

Abstract – *This paper presents the field of secure multi-party computation and Yao's Garbled Circuits protocol, which represents its basic implementation. It also descibes a secure ways of exchanging private data using the Oblivious Transfer protocols. The presented protocols were evaluated through an interactive graphical editor for the evaluation of logic circuits that adopts the previous concepts.*

Keywords: *MPC, 2PC, Yao's GC protocol, OT protocol, boolean circuit, interactive graphic editor*

1. UVOD

U vremenu konstantnog razvoja tehnologije, razmena podataka putem mreže postaje sve češća. Ipak, privatnost podataka koji se koriste prilikom različitih proračuna se sve više dovodi u pitanje. Manipulacije rezultatima aukcija i otkrivanje poverljivih ponuda, samo su neki od problema do kojih može doći ukoliko izračunavanja nad privatnim podacima nisu sigurna. U takvom okruženju, gde međusobno poverenje učesnika nije zagarantovano, javlja se potreba za razvojem mehanizama koji omogućavaju zajedničku obradu podataka uz zaštitu osetljivih informacija.

Zamislimo da dve osobe žele da saznaju ko ima više novca, ali bez otkrivanja svojih iznosa. Ovaj problem, poznat kao problem dva milionera (engl. *Two Millionaires Problem*) [1], zahteva računanje sa privatnim podacima uz očuvanje poverljivosti.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Milan Stojkov, docent.

Tradicionalni načini rešavanja ovog problema su podrazumevali angažovanje treće osobe od poverenja ili upotrebu različitih neefikasnih tehnika šifrovanja, što je zahtevalo velike resurse. Zbog toga je razvoj oblasti koja omogućava bezbedno i efikasno računanje nad osetljivim podacima od ključne važnosti za napredovanje mrežne bezbednosti.

Jedan od mehanizama koji teži da reši navedene probleme predstavlja grupa protokola za bezbedno izračunavanje sa više učesnika (engl. MPC - *Multi-Party Computation*) [2]. Primenjujući MPC protokole, obezbeđuje se privatnost podataka svih učesnika u različitim računskim procesima. U ovom radu posebna pažnja posvećena je Jaovom *Garbled Circuits* protokolu (Yao's GC), koji je od suštinskog značaja za razvoj MPC oblasti [3]. Ovaj protokol omogućava evaluaciju funkcija izraženih logičkim kolima u kojima interaguju dva učesnika (2PC). U radu će biti opisani i tipovi *Oblivious Transfer* (OT) potprotokola, koji igraju vitalnu ulogu u obezbeđivanju sigurnog prenosa podataka između učesnika u procesu evaluacija funkcija [4]. Takođe, kao glavni doprinos rada, evaluacija upotrebe opisanih protokola će biti urađena u interaktivnom grafičkom editoru koji igra ključnu ulogu u vizualizaciji i istraživanju sigurnosnih aspekata računanja, pružajući korisnicima intuitivno i efikasno okruženje za analizu i simulaciju kompleksnih logičkih kola.

2. BEZBEDNO IZRAČUNAVANJE SA VIŠE UČESNIKA

2.1. Definicija MPC

MPC je oblast kriptografije koja omogućava sigurno računanje u distribuiranim sistemima, efikasno štiteći podatke od zlonamernih učesnika. Osnovna definicija bezbednog izračunavanja se formalizuje kroz idealni svet. U idealnom svetu, učesnici šalju privatne podatke pouzdanoj trećoj strani, koja računa željenu funkciju i vraća rezultate. Iako ovaj pristup garantuje bezbednost, postojanje pouzdane treće strane ga čini imaginarnim. Umesto toga, učesnici međusobno komuniciraju koristeći unapred definisan protokol koji obezbeđuje da rezultati budu isti kao u idealnom svetu.

Prilikom razmatranja MPC važno je i precizno definisati ponašanje učesnika prilikom izračunavanja funkcija. Upravo tome služe dva osnovna modela bezbednosti: pasivni (engl. *semi-honest*) i aktivni (engl. *malicious*) [5].

U pasivnom modelu učesnici prate protokol, ali pokušavaju da naruše privatnost drugih učesnika. Sa druge strane, u aktivnom modelu bezbednosti, učesnici mogu da odstupe od protokola ili šalju pogrešne podatke kako bi narušili izračunavanje funkcije.

2.2. Osnovni MPC protokoli

Na temelju MPC oblasti su izgrađeni mnogi protokoli, a samo neki od njih su prikazani u Tabeli 1. Kako je prilikom odabira protokola važno da protokol bude što efikasniji, podaci o broju rundi i količini podataka koju je potrebno preneti prilikom evaluacije su prvi koji se upoređuju. Protokoli sa manjim brojem rundi i minimalnim komunikacionim troškovima su poželjniji, posebno u kompleksnim sistemima. Na primer, *Beaver-Micali-Rogaway* (BMR) protokol [11], koji koristi konstantan broj rundi, predstavlja značajan napredak u ovoj oblasti.

Tabela 1. *Osnovni MPC protokoli [5]*

Protokol	Broj učesnika	Broj rundi	Tip kola
Yao's GC	2	konstantan	logičko
GMW [12]	više od 2	dubina kola	logičko / aritmetičko
BGW [13]	više od 2	dubina kola	logičko / aritmetičko
BMR	više od 2	konstantan	logičko
GESS [14]	2	konstantan	logička formula

Oblast koja se razlikuje od opšteg slučaja sa više učesnika je MPC sa dva učesnika (engl. 2PC - *Two-Party Computation*) [6]. U ovom scenariju, dva učesnika mogu zajedno da izračunaju funkciju bez otkrivanja svojih privatnih podataka. Razvijen je veliki broj protokola koji omogućavaju ovaj oblik sigurne komunikacije, a jedan od najpoznatijih je Yao's GC protokol.

3. YAO'S GC PROTOKOL

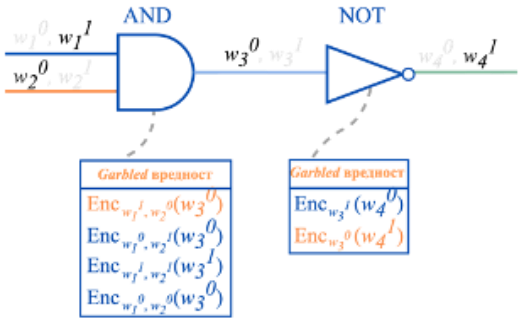
3.1. Klasičan Yao's GC protokol

Yao's GC protokol je jedan od najaktivnije proučavanih MPC metoda, inicijalno razvijen da podrži dva učesnika: *garbler*, u nastavku Alisa, koja formira *garbled* kolo i *evaluator*, odnosno Bob, koji izračunava izlaznu vrednost logičkog kola.

Osnovni koraci klasičnog Yao's GC protokola su sledeći:

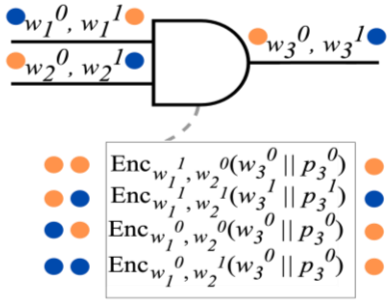
1) Alisa generiše logičko kolo za željenu funkciju f.
2) Alisa formira *garbled* kolo na osnovu logičkog kola tako što se za svaku logičku kapiju (engl. *gate*) šifruje tablica istinitosti. Ovaj proces obuhvata šifrovanje svakog podatka iz tablice istinitosti korišćenjem slučajno generisanih ključeva. Na samom kraju, redovi u formiranoj tabeli se permutuju kako se izlazna vrednost ne bi mogla odrediti na osnovu reda u tabeli.
3) Alisa šalje Bobu formirano *garbled* kolo, zajedno sa šifrovanim vrednostima svojih ulaza.
4) Bob pomoću OT protokola od Alise dobija podatke o šifrovanim vrednostima svojih ulaza, bez otkrivanja privatnih podataka. Opis OT protokola je prikazan u narednoj sekciji 3.2.
5) Bob evalira logičko kolo tako što prolazi kroz sve logičke kapije i pokušava da dešifruje redove u njihovim garbled tabelama. Ukoliko je protokol uspešno sproveden, Bob za svaku tabelu uspeva da pročita tačno jedan red.

Uprošćen prikaz evaluacije logičkog kola je dat na slici 1.



Slika 1. *Prikaz evaluacije logičkog kola. Ulazna vrednost koju unosi Alisa na žici w_1 je 1, dok je Bob na žicu w_2 uneo 0. Prvi red u levoj i drugi red u desnoj garbled tabeli su označeni kao uspešno dešifrovani redovi.*

Kako prethodno opisan klasičan Yao's GC protokol nije efikasan u realnim uslovima, vremenom su se razvile različite tehnike optimizacije [7, 8]. One se fokusiraju na smanjenje veličine *garbled* kola i broja funkcija koje se pozivaju tokom evaluacije. Jedna od ključnih tehnika optimizacije je *point-and-permute* [8]. Ona omogućava Bobu da utvrdi koju šifrovanu vrednost treba da dešifruje, bez potrebe da dešifruje sve četiri vrednosti kao kod klasičnog protokola. Ovo se postiže dodavanjem nasumičnog selekcionog bita svakoj žici. Na slici 2 se vidi da šifrovane vrednosti za ulaze imaju pridružene slučajne bitove. Oni služe da se na osnovu njih indeksira tablica istinitosti. Na ovaj način se smanjuje broj nepotrebnih operacija i ubrzava proces jer Bob tokom evaluacije tačno zna koji red treba da dešifruje.



Slika 2. *Prikaz formiranja garbled kola korišćenjem point-and-permute tehnike sa p selekcionim bitom*

3.2. OT protokol

U mnogim protokolima bezbednog izračunavanja postoji potreba da jedna strana dobije informacije od druge bez otkrivanja suvišnih podataka. Ovo proizilazi iz činjenice da je danas malo prostora za potpuno poverenje između učesnika prilikom komunikacije. Zbog toga je potreban protokol koji će omogućiti diskretnu razmenu informacija. OT pruža siguran način razmene podataka uz minimalno otkrivanje informacija [9].

U osnovi OT protokol ima tri varijante [4]:

- *1-out-of-2* je verzija u kojoj učestvuju dve strane. Primalac na kraju protokola saznaje jednu od dve

ulazne vrednosti koje poseduje pošiljalac, pri čemu pošiljalac ne zna ništa o izboru primaoca.

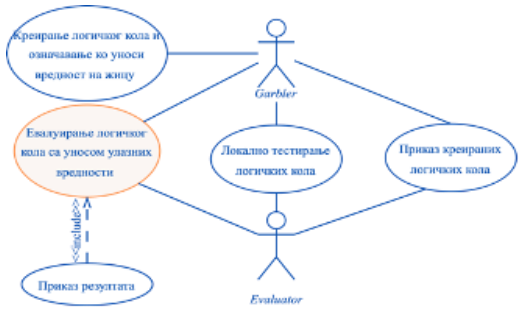
- *1-out-of-n* je proširena verzija *1-out-of-2* OT protokola koja omogućava jednoj strani, odnosno primaocu da dobije jedan od nekoliko podataka koje poseduje druga strana. Takođe, pošiljalac ne dobija informaciju o izboru primaoca.
- *k-out-of-n* omogućava jednoj strani, odnosno primaocu da dobije više podataka od druge strane, pri čemu pošiljalac ima nekoliko ulaznih podataka. Na kraju protokola, primalac saznaje onoliko vrednosti koliko je izabrao, dok pošiljalac ne dobija nikakvu informaciju o izboru primaoca.

4. SPECIFIKACIJA GRAFIČKOG EDITORA

Cilj interaktivnog grafičkog editora za evaluaciju *Garbled Circuits* protokola je da korisnicima omogući intuitivno kreiranje i analizu logičkih šema. Ovako kreirane logičke šeme se koriste u protokolu bezbednog izračunavanja sa dva učesnika.

4.1. Specifikacija funkcionalnosti

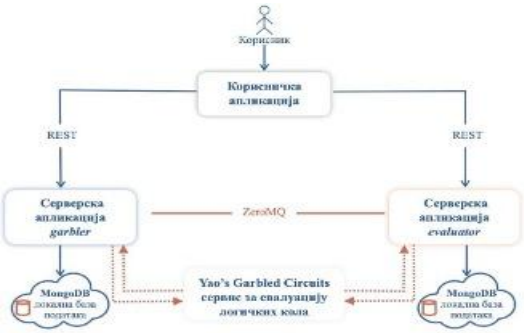
Dijagram slučajeva korišćenja je najjednostavniji način specifikacije šta određeni učesnici mogu da izvrše u posmatranom sistemu. Na slici 3 je prikazan dijagram slučajeva korišćenja za editor evaluacije logičkih kola, koji obuhvata dve ključne uloge: *garbler* i *evaluator*. *Garbler* može da kreira logičko kolo i bira učesnika koji će tokom evaluacije da unosi vrednost na datu žicu. Obe uloge mogu da pregledaju i lokalno testiraju logičko kolo, a nakon toga *evaluator* može da započne evaluaciju logičkog kola. Takođe, učesnici imaju i mogućnost pregledanja dobijenih rezultata evaluacije.



Slika 3. *Dijagram slučajeva korišćenja*

4.2. Specifikacija sistema

Glavne komponente interaktivnog grafičkog editora za evaluaciju *Garbled Circuits* protokola su prikazane na slici 4.



Slika 4. *Arhitektura interaktivnog grafičkog editora za evaluiraciju Garbled Circuits protokola*

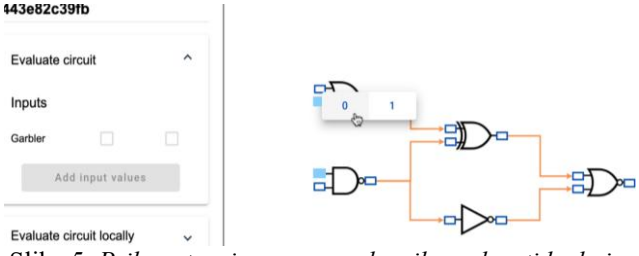
Korisničku interakciju sa sistemom omogućava aplikacija implementirana u *Angular 18* radnom okviru. Fokus ove aplikacije je na formiranju okruženja koje će korisnicima ponuditi jednostavno kreiranje, pregled i evaluaciju logičkih kola. Nakon odabira željene funkcionalnosti, poziva se metoda određenog servisa serverske aplikacije, a komunikacija se odvija putem HTTP protokola.

Serverske aplikacije su implementirane pomoću *Spring Boot 3* radnog okvira. *Garbler* serverska aplikacija predstavlja modul za kreiranje *garbled* verzije logičkog kola, koja se čuva u lokalnoj *MongoDB* bazi podataka. Server za evaluiranje kola komunicira sa Yao's GC servisom, omogućavajući izračunavanje logičkog kola bez otkrivanja osetljivih informacija. Komunikacija između servera se u realnom vremenu, bez dodatnog nadzora mreže, odvija preko *ZeroMQ* sistema poruka [10].

Nakon što je opisan proces razmene podataka između komponenti, važno je naglasiti da sistem treba da omogući jednostavno dodavanje novih protokola za izračunavanje logičkih kola, bez remećenja postojećih funkcionalnosti. Iz tog razloga, arhitektura sistema je dizajnirana da bude proširiva, sa protokolima implementiranim u zasebnim modulima koji komuniciraju putem zajedničkog interfejsa. Ovakav pristup obezbeđuje fleksibilnost sistema i olakšava buduće nadogradnje bez ugrožavanja stabilnosti.

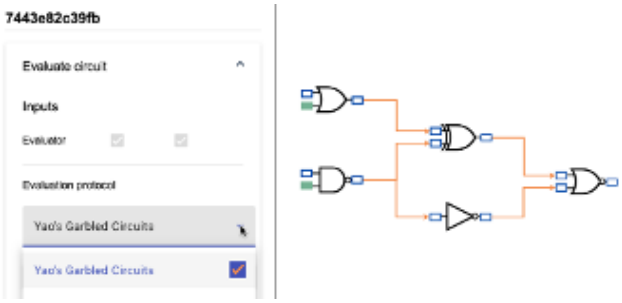
5. IMPLEMENTACIJA GRAFIČKOG EDITORA

Osnovna funkcionalnost interaktivnog grafičkog editora za evaluaciju *Garbled Circuits protokola* je evaluacija izabranog logičkog kola. Proces počinje unosom binarnih vrednosti na ulazne žice prvog sloja kapija, pritiskom na pravougaonike i izborom vrednosti. Stranica je prikazana na slici 5.



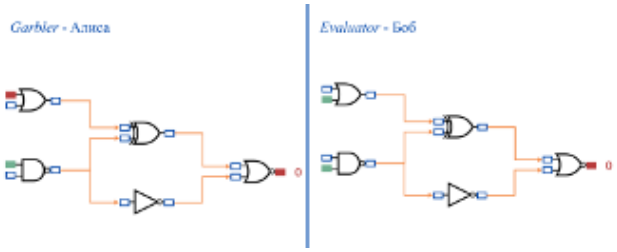
Slika 5. *Prikaz stranice za unos ulaznih vrednosti kada je pregleda garbler*

Kada Alisa uspešno unese vrednosti na ulazne žice, omogućava se pokretanje evaluacije logičkog kola. Tada Bob dobija mogućnost da učestvuje u evaluaciji logičkog kola. Na slici 6 je prikazana stranica za unos i pokretanje evaluacije logičkog kola kada je pregleda *evaluator*. Proces dodavanja ulaznih vrednosti se obavlja na isti način kao što to radi i Alisa. Bob, za razliku od Alise, ima opciju da bira po kom protokolu će biti vršeno evaluiranje datog logičkog kola. Trenutno, sistem podržava evaluaciju korišćenjem klasičnog Yao's GC protokola koji je opisan u poglavlju 3.1.



Slika 6. *Prikaz stranice za slanje unetih ulaznih vrednosti kada je pregleda evaluator*

Po završetku evaluacije logičkog kola, oba učesnika dobijaju obaveštenje o tome, pri čemu nijedna strana na kraju nije svesna ulaznih vrednosti koje je suprotna strana odabrala. Poređenje stranica za prikaz rezultata kod oba učesnika se nalazi na slici 7.



Slika 7. *Prikaz rezultata uspešnog evaluiranja logičkog kola*

6. ZAKLJUČAK

U ovom radu je predstavljeno rešenje za kreiranje interaktivnog grafičkog editora za evaluaciju *Garbled Circuits* protokola. Kako je akcenat na sigurnosti podataka sve značajniji, odatle proizilazi potreba da se omogući grupi nezavisnih učesnika koji ne veruju jedni drugima ili bilo kojoj trećoj strani, da bezbedno izračunaju funkciju koja zavisi od njihovih privatnih ulaza. Ovaj editor predstavlja rešenje koje olakšava vizualizaciju i manipulaciju logičkim kolima, istovremeno implementirajući principe bezbednog izračunavanja.

U radu su prvo opisane teorijske osnove MPC oblasti i predstavljen Yao's GC protokol. Opisani su i OT protokoli, koji omogućavaju primaocu da dobije jednu od ulaznih vrednosti koje poseduje druga strana, dok pošiljalac ne saznaje nikakve informacije o izboru primaoca. Na ovaj način je ukazano na mogućnost stvaranja sigurnog digitalnog ekosistema za obradu logičkih kola, gde su svi podaci zaštićeni tokom prenosa i obrade. Ovakav sistem obezbeđuje saradnju između učesnika bez rizika od narušavanja privatnosti. Specifikacija sistema je prikazana u nastavku rada, dok je na kraju opisana konkretna implementacija funkcionalnosti evaluiranja logičkog kola.

Koraci daljeg razvoja platforme za evaluaciju kola uključuju implementaciju različitih tehnika optimizacije klasičnog Yao's GC протокола, kao i drugih protokola koji koristi logička kola. Takođe, ukoliko bi se interaktivni grafički editor posmatrao kao mesto daljeg razvoja, može se razmotriti kreiranje editora koji bi obezbedio više mogućnosti za manipulaciju logičkim kapijama i žicama između njih. Ovo bi korisnicima omogućilo veću fleksibilnost u kreiranju i modifikaciji logičkih šema, čime bi se unapredila njihova interakcija sa platformom.

7. LITERATURA

[1] Boudot, F., Schoenmakers, B., & Traore, J. (2001). A fair and efficient solution to the socialist millionaires' problem. Discrete Applied Mathematics, 111(1-2), 23-36.
[2] Lindell, Y. (2020). Secure multiparty computation. Communications of the ACM, 64(1), 86-96.
[3] Lindell, Y., & Pinkas, B. (2009). A proof of security of Yao's protocol for two-party computation. Journal of cryptology, 22, 161-188.
[4] Yadav, V. K., Andola, N., Verma, S., & Venkatesan, S. (2022). A survey of oblivious transfer protocol. ACM Computing Surveys (CSUR), 54(10s), 1-37.
[5] Evans, D., Kolesnikov, V., & Rosulek, M. (2018). A pragmatic introduction to secure multi-party computation. *Foundations and Trends® in Privacy and Security*, *2*(2-3), 70-246.
[6] Malkhi, D., Nisan, N., Pinkas, B., & Sella, Y. (2004, August). Fairplay-Secure Two-Party Computation System. In USENIX security symposium (Vol. 4, p. 9).
[7] Yakoubov, S. (2017). A gentle introduction to yao's garbled circuits. Dostupno na https://web. mit. edu/sonka89/www/papers/2017ygc.pdf (datum pristupa 10-09-2024)
[8] Beaver, D., Micali, S., & Rogaway, P. (1990, April). The round complexity of secure protocols. In Proceedings of the twenty-second annual ACM symposium on Theory of computing (pp. 503-513).
[9] Rabin, M. O. (2005). How to exchange secrets with oblivious transfer. Cryptology ePrint Archive.
[10] Hintjens, P. (2013). *ZeroMQ: Messaging for Many Applications*. O'Reilly Media.
[11] Beaver, D., Micali, S., & Rogaway, P. (1990, April). The round complexity of secure protocols. In Proceedings of the twenty-second annual ACM symposium on Theory of computing (pp. 503-513).
[12] Goldreich, O., Micali, S., & Wigderson, A. (2019). How to play any mental game, or a completeness theorem for protocols with honest majority. In Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali (pp. 307-328).
[13] Ben-Or, M., Goldwasser, S., & Wigderson, A. (2019). Completeness theorems for non-cryptographic fault-tolerant distributed computation. In Providing sound foundations for cryptography: on the work of Shafi Goldwasser and Silvio Micali (pp. 351-371).
[14] Kolesnikov V., (2005). Gate evaluation secret sharing and secure one-round two-party computation, Advances in Cryptology-ASIACRYPT.

Kratka biografija:

Zorica Vuković rođena je u Sremskoj Mitrovici 2000. godine. Osnovne akademske studije je završila 2023. godine na Fakultetu tehničkih nauka u Novom Sadu. Master rad na Fakultetu tehničkih nauka iz oblasti Softversko inženjerstvo – Elektronsko poslovanje odbranila je 2024. godine.