Hiter protokol miselnega pokra

Aljaž Erzin

ae1814@student.uni-lj.si

Povzetek. V članku bomo predstavili hiter in zanesljiv protokol miselnega pokra. Osnovna struktura bo podobna Barnett & Smartovem in Castella-Rocovem protokolu, z določenimi spremembami šifrirnih shem. Protokol, ki ga bomo predstavili je dvakrat hitrejši od omenjenih. Zaradi hitrejših osnovnih protokolov (mešanje vseh kart) bomo izboljšali hitrost mešanja podmnožice kart med trenutno rundo. Sledi, tako pri našem kot tudi pri drugih načinih, da pohitritev določenega dela protokola pomeni upočasnitev drugega dela. Zato je izbira protokola odvisna tudi od pravil igre. Ker je naš protokol hiter pri mešanju kart, pri večkratnem mešanju sredi runde pa počasen, je uporaben predvsem za igre kot so Poker, Tarok, Blackjack...

Ključne besede: miselni poker, mešanje, karte, protokol, odločitvena Diffie-Hellmanova predpostavka (angl. decision Diffie-Hellman assumption, kratica DDH), dokaz brez razkritja znanja (angl. zero knowledge proof, kratica ZKP), problem diskretnega logaritma (angl. discrete logarithm problem, kratica DLP)

1 UVOD

Kriptografski problem miselnega pokra je zanimiv način vzpostavitve pravičnega sistema igranja iger na daljavo, brez zaupanja vredne tretje osebe. Večino iger prek spleta poteka z dodatnim, zaupanja vrednim centralnim strežnikom. Pogosto se zgodi, da igralci ne zaupajo strežnikom ali pa si želijo igranja brez dodatne osebe/strežnika. Naša naloga je, da igralcem omogočimo hitro in varno igro, brez goljufij in medsebojnega sodelovanja. Ker tudi pri igrah v živo osebe lahko goljufajo, si prizadevamo, da vzpostavimo sistem, ki bo varen vsaj toliko, kot je varen sistem igranja v realnem življenju. Takšen sistem imenujemo protokol miselnega pokra. Poleg varnosti moramo biti pozorni tudi na časovno zahtevnost protokolov. Želimo imeti hitre šifrirne algoritme. Skozi članek bomo spoznali, da težko pohitrimo del protokola, brez upočasnitve drugega dela. To dejstvo nas vodi do ugotovitve, da se pred izbiro protokola pozanimamo o sami igri, koliko igralcev bo igralo, se pri posamezni rundi uporabljajo vse karte ali le del, je potrebno večkratno mešanje kart... ter nato izberemo najbolj primeren protokol.

Za boljšo predstavo, kaj miselni poker je, vzemimo preprost primer igre s kartami. Anita in Bojan premešata 10 kart, ki so označene s številkami od 1 do 10. Vsak vzame 2 karti iz kupa. Zmagovalec je tisti, ki ima večjo vsoto številk na kartah. Ker igralca nista v istem prostoru, karte najprej premeša Bojan, vsako karto zašifrira s svojim zasebnim ključem (naključnim številom), pošlje zašifrirane karte Aniti, ki ponovi enak postopek. Na tem mestu nihče ne pozna vrstnega reda kart. V naslednjem koraku vzameta vsak po dve karti iz vrha šifriranega kupčka. Bojan pošlje izvlečeni karti Aniti, ki jih odklene s svojim zasebnim ključem, ter jih pošlje nazaj Bojanu. Bojan potem odklene ti dve karti s svojim zasebnim ključem. Enak postopek naredita še v obratni smeri. Sedaj oba poznata karti v svoji roki in lahko preverita, kdo je zmagovalec igre.

Kriptografski protokoli na tem področju so se pričeli razvijati z idejo poštenega metanja kovanca na daljavo. Recimo, da Anita in Bojan igrata igro metanja kovancev. Normalna igra v živo bi potekala tako, da Anita izbere stran kovanca (cifra ali grb), Bojan kovanec vrže in obrne. Če je Anita izbrala grb in je na kovancu grb, je zmagala ona, drugače je zmagovalec Bojan. Težava se pojavi, če Anita in Bojan nista v istem prostoru. Po tem, ko je Anita izbrala stran kovanca, lahko Bojan goljufa ter rezultat meta obrne sebi v prid. Podobno, če Anita ne objavi svoje izbire strani kovanca Bojanu, potem ko Bojan obrne kovanec in objavi rezultat, lahko Anita trdi, da je izbrala stran kovanca, ki ji prinese zmago. Da bi preprečili možnost goljufanja, je Manuel Blum vpeljal zavezujočo shemo (šifrirano izbiro kovanca bomo imenovali zaveza). Ta omogoča Aniti, da objavi svojo izbiro strani kovanca Bojanu, brez da bi (do konca igre) razkrila svojo dejansko izbiro. Tako bo Anita lahko izbrala stran kovanca ter objavila zavezo izbire Bojanu. Ker Bojan ne pozna prave strani kovanca (strani, ki jo je izbrala Anita), tudi sam ne more goljufati. Bojan zato objavi rezultat meta, Anita razkrije svojo zavezo, nato oba preverita rezultat.

Skozi čas je nastalo kar nekaj različnih protokolov miselnega pokra. V našem članku bomo primerjali spodaj predstavljen protokol miselnega pokra z Barnett & Smartovim in Castella-Rocovim protokolom, kjer oba uporabljata osnove ElGamalove šifrirne sheme. Protokola se razlikujeta predvsem v hitrosti, Castella-Rocovo mešanje kart je hitrejše od Barnett & Smartovega.

Predstavili bomo hiter in varen protokol miselnega pokra za mešanje kart. Protokol je podoben Barnett & Smartovemu ter Castella-Rocovemu. Razlika je le v postopku šifiriranja/odšifriranja kart. V omenjenih dveh protokolih vsak izmed igralcev uporablja dva različna zasebna ključa za mešanje kart. Enega za šifriranje kart, drugega za mešanje (permutiranje) kart. Naš protokol se od zgoraj omenjenih protokolov razlikuje po tem, da uporablja samo en zasebni ključ za celoten proces mešanja. Ta isti ključ se uporablja tudi za odšifriranje kart. Ker pri našem protokolu uporablja vsak igralec le en zasebni ključ, pri drugih pa dva, ugotovimo, da je pri mešanju celotnega kupa kart, naš protokol dvakrat hitrejši od omenjenih. Na račun hitrejšega mešanja kart, pa izgubimo na hitrosti pri ponovnem mešanju podmnožice vseh kart. Pri protokoloma (Castella-Roccov in Barnett & Smartov protokol) zaradi uporabe drugega zasebnega ključa igralci lahko šifrirajo le določeno podmnožico kart. V našem primeru pa vsako mešanje zahteva šifriranje vseh kart z novim zasebnim ključem. Zaradi te lastnosti je naš protokol namenjen predvsem igram, kjer se karte premešajo le na začetku igre. V nadeljevanju protokol razdelimo na več delov:

1) priprava kupa kart,
2) mešanje kart,
3) izbira (vlečenje) kart iz kupa,
4) odpiranje kart.

Proti koncu članka bomo podali še komentar o varnosti in časovni zahtevnosti protokola ter kdaj in zakaj ga je smiselno uporabiti. Za zaključek pa bomo nekaj besed namenili še prihodnosti in odprtim problemom miselnega pokra v splošnem.

2 VSEBINA PROTOKOLA

V članku uporabimo več znanih kriptografskih konceptov in načinov šifriranja:

1) Problem diskretnega logaritma (angl. discrete logarithm problem, kratica DLP) opisuje kompleksnost rešitve enačbe $\log_a b = x$. Se pravi iščemo vrednost x, da bo veljalo $a^x = b$. V večini primerov je takšen x zelo težko najti. Zato bomo v našem protokolu igralne karte šifrirali tako, da bo vsak igralec karti dodal eksponent (svoj zasebni ključ). Varnost našega protokola sloni na varnosti DLP.
2) Karte predstavimo z naključnimi števili iz ciklične grupe G ($A_i \in G$). Igralec i za šifriranje uporablja svoj zasebni ključ X_i. Sledi, da je karta A_i zašifrirana v $Y_i = A_i^{X_i}$. Isti zasebni ključ X_i se uprablja tudi pri odšifriranju karte.
3) Odločitvena Diffie-Hellmanova predpostavka (angl. decision Diffie-Hellman assumption, kratica DDH). Naj bo G neka ciklična grupa, Γ pa družina cikličnih grup. Za katerikoli generator $g \in G \in \Gamma$ ter a, b in c (naključne vrednosti naravnih števil), je DDH predpostavka za Γ, da sta naslednji četverici enaki (kjer je grupa G končna):
$$(g, g^a, g^b, g^{(ab)}) \text{ in } (g, g^a, g^b, g^c)$$
4) **Dokaz brez razkritja znanja** (angl. zero knowledge proof, kratica ZKP) je protokol, ki vsebuje dve osebi, dokazovalca (recimo ji Vera) in preveritelja (recimo mu Primož). Veri omogoča, da Primožu dokaže, da je določena izjava resnična, ne da bi pri tem izdala kakršnokoli informacijo o tem, kako dejstvo dokazati.
Definicija: Naj bo Π odločitveni problem. Imamo protokol med Primožem in Vero, v katerem Primož najprej poda verjetnostni izziv (Π, x), Vera pa nanj odgovori. Primož odgovor interpretira kot dokaz in ga sprejme ali zavrne, glede na to, ali je $x \in \Pi$. Tak protokol je interaktivni dokaz za problem Π, če veljata naslednji lastnosti
   - **polnost**: tj. če $x \in \Pi$, Primož vedno sprejme dokaz.
   - **uglašenost**: tj. če $x \notin \Pi$, Primož sprejme dokaz z verjetnostjo, manjšo od $\frac{1}{2}$(Trampuš, 2008)[5].

Primer: Recimo, da je Primož barvno slep, Vera pa lahko vidi barve. Imamo dve kroglici enake oblike, eno rdečo in eno zeleno. Primožu se zdita enaki in Veri ne verjame, da sta res različni. Vera mu želi dokazati, da sta različno obarvani, vendar mu pri tem ne želi razkriti katera kroglica je rdeče in katera zelene barve. Tu Veri pomaga ZKP. Obe kroglici da Primožu, on pa ju skrije za hrbet. Nato vzame eno od kroglic in jo pokaže Veri, ter jo spet skrije za hrbet. Potem se odloči, ali bo Veri ponovno pokazal isto kroglico ali pa ji bo pokazal drugo, pri čemer bo z enako verjetnostjo izbral eno od kroglic. Vero bo za tem vprašal ali je zamenjal kroglico. Celoten postopek bo ponovil tako pogosto, kot je potrebno. Če Vera res vidi barvo kroglic lahko z gotovostjo trdi, ali je Primož kroglici zamenjal ali ne. Po drugi strani pa, če bi bili kroglici enake barve in s tem nerazločljivi, Vera ne bi mogla pravilno uganiti z verjetnostjo večjo od $\frac{1}{2}$. Tako lahko, če večkrat ponovimo ta dokaz, Vera z gotovostjo prepriča Primoža, da sta kroglici različne barve. Zgornji dokaz je

dokaz brez razkritja znanja, saj Primož nikoli ne izve, katera kroglica je rdeča in katera zelena, oz. povedano drugače, ne pridobi znanja o tem kako razločiti kroglici.

2.1 Priprava kupa kart

Osredotočimo se na igro z M kartami, ki jo igra N igralcev. Naj bo $G \in \Gamma$ (ciklična grupa, poljubno velikega reda, ki zadošča DDH predpostavki). Karte predstavimo s števili i $(1 \leq i \leq M)$ - nobeni dve različni karti nimata istega pripadajočega števila. Za vsako karto i, igralci generirajo naključna različna števila $A_i \in G$.

1 Algoritem za pripravo kupa kart

1) Igralci generirajo različne neodvisne naključne generatorje $A_i \in G$ za vsak $0 \leq i \leq M$ z uporabo algoritma za generiranja naključnega elementa.
2) Zapredje $(A_i)_{0 \leq i \leq M}$ predstavlja naš kup kart.

2 Algoritem za generiranje naključnega elementa

1) Za vsak $j = 1, \ldots, N$ igralec j naredi sledeče:
   a) naključno izbere generatorja $g_j, h_j \in G$ ter naključno število $\lambda_j > 0$,
   b) naj bo $g'_j = g_j^{\lambda_j}$,
   c) objavi g_j, g'_j, h_j.
2) Za vsak $j = N, \ldots, 1$ igralec j naredi sledeče:
   a) naj bo $h'_j = h_j^{\lambda_j}$,
   b) objavi h'_j,
   c) uporabi ZKP, da ostale igralce prepriča, da velja $\log_{g_j} g'_j = \log_{h_j} h'_j$.
3) Vrne rezultat $h = \prod h'_j$.

Generatorje A_i lahko dobimo z algoritmom za generiranje naključnega elementa. Pozorni moramo biti na to, da bo vrednost iz ciklične grupe G, ter da bodo generirana števila med seboj različna. Lahko vzamemo grupo G kvadratičnih ostankov z velikim praštevilom oblike $p = 2q + 1$ (kjer je q praštevilo), ali pa za G uporabimo eliptično krivuljo nad $\mathbb{Z}_p$...

2.2 Mešanje kupa

Kup je pravilno premešan, ko se spremeni le vrstni red kart (permutacija kart). Nepremešan kup kart označimo z B_0. Igralec 1 premeša kup B_0, novo premešan kup označimo z B_1. V vsaki naslednji iteraciji spodnjega algoritma igralec j prejme premešan kup B_{j-1}, ko ga premeša še on, dobimo premešan kup z oznako B_j. Potek algoritma je naslednji:

3 Algoritem za mešanje kupa kart

1) Naj bo $B_0 = (b_{0,i})_{i=1}^M$, kjer je $b_{0,i} = a_i$.
2) Za $j = 1, \ldots, N$, zaporedoma, igralec j naredi naslednje:
   a) naključno izbere zasebni ključ x_j $(0 < x_j < p)$,
   b) naključno izbere tako permutacijo π_j elementov množice $\{1, 2, \ldots, M\}$, da velja $\pi_j(0) = 0$,
   c) izračuna $B_j = (b_{j,i})_{i=1}^n$, kjer je $b_{j,i} = b_{j-1,\pi(i)}^{x_j}$
   d) objavi B_j vsem igralcem,
   e) uporabi preverjanje pravičnosti mešanja kart, da prepriča ostale igralce, da je kup B_j premešan brez goljufanja.
3) $B = B_N = (b_{N,i})_{i=1}^M$ je premešan kup.

Preverjanje pravičnosti mešanja kart se izvede podobno kot dokaz brez razkritja znanja (ZKP). Preverjanje nam vrne odgovor, ali je igralec j pošteno premešal kup. Če igralec ne prestane testa preverjanja mešanja, je takoj izključen iz igre. Algoritem preverjanja poteka tako, da igralec j (trenutni mešalec) generira K različnih eksponentov (pri tem ne uporablja svojega zasebnega ključa x_j) in permutacij vrednosti $b_i \in B$. Nato skupaj z drugimi igralci (s pomočjo metode ZKP) potrdijo pravično mešanje kart (med preverjanjem mora igralec j uporabiti tudi svoj zasebni ključ, saj bodo le tako lahko potrdili pravičnost). Algoritem zapišemo kot:

4 Algoritem za preverjanje pravilnosti mešanja kart

1) Igralec j naključno izbere števila $0 < y_1, y_2, \ldots, y_K < p$.
2) Igralec j naključno izbere permutacije $\pi'_1, \pi'_2, \ldots, \pi'_K$ množice $(0, 1, 2, \ldots, M)$.
3) Igralec j izračuna $C_k = (c_{k,i})_{0 \leq i \leq M}$, kjer je $c_{k,i} = b_{j,\pi'_k(i)}^{y_k}$ za $k = 1, 2, \ldots, K$.
4) Za vsak $k = 1, \ldots, K$:
   a) Igralec j objavi C_k.
   b) Ostali igralci zgenerirajo bitno število e_k s pomočjo algoritma za generiranje naključnega elementa.
   c) Igralci pošljejo e_k igralcu j.
   d) Če je $e_k = 0$, igralec j objavi y_k, π'_k in vsak igralec izračuna $d_{k,i} = b_{j,\pi'_k(i)}^{y_k}$ za vsak i.
   e) Če je $e_k = 1$, igralec j objavi $x_k y_k, \pi_j \pi'_k$ in vsak igralec izračuna $d_{k,i} = b_{j-1,\pi_j \pi'_k(i)}^{x_k y_k}$ za vsak i.
   f) Če za katerikoli i, $d_{k,i} \neq c_{k,i}$, potem igralec j ne prestane preverjanja pravilnosti mešanja.
5) Igralec j prestane preverjanje pravilnosti mešanja.

Spremenljivka K je vnaprej izbrano število ponovitev preverjanja. Večji kot je, večja je verjetnost, da bo preverjanje vrnilo pravilen odgovor.

2.3 Vlečenje kart in odpiranje s karto

Algoritem za vlečenje lahko opišemo na naslednji način:

5 Algoritem za vlečenje kart

1) Igralec j_0 izbere karto $c_0 \in B$ in jo objavi v javni kanal.
2) Vsi igralci zaporedoma $(j = 1, 2, \ldots, N)$ naredijo sledeče:
   a) izračunaj $c_j = c_{j-1}^{x_j^{-1}}$,
   b) objavi c_j,
   c) s pomočjo ZKP prepričaj ostale igralce, da je c_j res izračunan iz predhodnega c_{j-1}.
3) Igralec j_0 izračuna $c = c_N^{x_0^{-1}}$, ter najde tak i, za katerega drži $A_i = c$. Karta i je izvelečena karta.

Ko izvleče karto, mora igralec j_0 še dokazati ostalim, da je karta i res karta, ki jo izvlekel.

6 Algoritem za odpiranje kart

Igralec j_0 trdi, da ima karto i ter uporabi ZKP, da ostale igralce prepriča o pravilnosti enačbe $\log_{A_i} c_N = \log_{b_{j_0-1,0}} b_{j_0}$.

2.4 Ponovno in delno mešanje

Kup ponovno mešamo po istem načinu kot v točki *2.2 - Mešanje kupa*. Le da tokrat mešamo B (premešani kup), vsak igralec pa uporabi nov zasebni ključ x'_j $(0 \leq j \leq N)$. To nam poveča čas odšifriranja kart, saj mora vsak izmed igralcev karto odšifrirati z dvema zasebnima ključema, x_j in x'_j. Sam algoritem vlečenja kart ostaja podoben opisanemu, le da vsak igralec odšifrira trenutno karto z vsemi svojimi zasebnimi ključi.

Delno mešanje kart je, kot smo že omenili, v našem protokolu časovno bolj zahtevno kot pri drugih. Uporabimo sicer protokol mešanja kart iz podpoglavja *Mešanje kart*, s tem da permutiramo le del kart, ki ga želimo premešati. Še vedno pa moramo uporabiti nov zasebni ključ x_j (drugačen od do sedaj uporabljenih) na vseh kartah.

3 Analiza varnosti in učinkovitosti

3.1 Varnost

Omenili smo, da si želimo sistem, ki je pravičen vsaj toliko, kot je lahko pravična navadna igra, kjer so igralci v istem prostoru. Tudi pri takih igrah obstaja medsebojno povezovanje igralcev, skrivno gledanje kart soigralcu in podobno.

Z igro na daljavo ter vpeljavo protokola miselnega pokra (brez uporabe zaupanja vredne osebe), smo določene nepravičnosti odpravili (npr. gledanje v karte), nekaterih pa ni bilo moč odpraviti tudi z vpeljavo kriptografskih protokolov.

Ena od možnih oblik goljufij je medsebojna komunikacija posameznih igralcev, kjer lahko zlahka oblikujejo različne oblike sodelovanj in s tem igrajo nepravično igro. Odprava ali omejevanje zasebnih kanalov med igralci dandanes še vedno ostaja ostaja dokaj nerazvit problem, v katerega pa se ne bomo podrobneje spuščali.

Med drugim je v miselnem pokru po zgledu mnogih drugih kriptografskih shem popularno šifriranje kart s pomočjo potenciranja: karto z znanim čistopisom x igralec zašifrira tako, da jo s svojim zasebnim ključem e pretvori v x^e. Če to naredi za vse karte, nato pa dobljene vrednosti še permutira med seboj, preden jih objavi, soigralci ne znajo več povezati tajnopisov s čistopisi. Problem diskretnega logaritma od nas zahteva, da znotraj multiplikativne grupe G, za dani $\alpha, \beta \in G$, kjer je red α enak n, najdemo $x \in 1, \ldots, n-1$ za katerega velja $\alpha^x = \beta$. Povedano drugače, iščemo logaritem: $x = \log_\alpha \beta$. Problem diskretnega logaritma je domnevno težko rešljiv, zato je naš sistem šifriranja posledično varen.

To je osnovna ideja, ki se izvaja tudi v predstavljenem protokolu ter spada med napogostejše izvedbe mešanja kart v miselnem pokru. Ker je DLP (problem diskretnega logaritma) izrazito baziče problem, v implementacijah mislenega pokra nastopa tudi kot gradnik različnih protokolov. Na njem je na primer osnovan marsikateri dokaz brez razkritja znanja, konstrukt, ki zelo olajša snovanje miselnega pokra brez zaupanja vredne tretje osebe (Trampuš, 2008)[5].

3.2 Učinkovitost

V tem razdelku se bomo osredotočili na primerjavo časovne zahtevnosti protokola z dvema drugima protokoloma in sicer s Castella-Rocovim in Barnett & Smartovim.

Z namenom, da bi protokole čim bolj točno primerjali, smo za najbolj časovno potratne operacije uporabili posebne oznake. Časovno zahtevnost izračuna dokaza brez razkritja znanja smo označili s črko Z, potenciranja s črko e in množenja s črko m. Časovne zahtevnosti drugih operacij so bile precej nižje in smo jih zaradi boljše preglednosti zanemarili. Predpostavimo, da opazujemo igro, ki jo igra N igralcev s kupom M kart.

3.2.1 Časovna zahtevnost mešanja kart: Mešanje kart je običajno najbolj zamuden del protokola miselnega

pokra. Tu se spomnimo na poglavje *2.2 Mešanje kupa* in spremenljivke K, ki predstavlja vnaprej izbrano število ponovitev preverjanja.

	Časovna zahtevnost mešanja
Protokol miselnega pokra	$(KN+1)(m+1)Ne+\frac{1}{2}KNm$
Castella-Rocca	$2(KN+1)MNe+\frac{1}{2}KMNm$
Barnett&Smart	$2(KN+1)MN(e+m)+Mm$

Tabela 1: Časovna zahtevnost mešanja kupa kart

Mešanje pri predstavljenem protokolu je približno dvakrat hitrejše v primerjavi z drugimi protokoli. Če bi časovno zahtevnost množenja m nastavili na 0, bi imela protokola Castella-Rocca in Barnett&Smart enako časovno zahtevnost. Glavna pomanjkljivost protokola je povezana z delnim mešanjem kupa kart. Pri protokolih Castella-Rocca in Barnett & Smart je časovna zahtevnost za premešanje podmnožice kart, ki vsebuje S kart, $\frac{S}{M}$-kratnik časovne zahtevnosti mešanja celotnega kupa. V nasprotju z omenjenima protokoloma je časovna zahtevnost delnega mešanja kart z uporabo našega protokola enaka mešanju celotnega kupa. Torej za igre s kartami, ki vsebujejo veliko vmesnih delnih mešanj, naš protokol ni primeren. Kljub tej pomanjklivosti, pa je več kot ustrezen za igre s kartami, katere vmesnega mešanja ne vsebujejo.

3.2.2 Časovna zahtevnost odpiranja in vlečenja kart: Po drugi strani pa je časovna zahtevnost odpiranja in vlečenja kart veliko nižja v primerjavi s časovno zahtevnostjo mešanja.

	Časovna zahtevnost odpiranja
Protokol miselnega pokra	Z
Castella-Rocca	$Z+(N-1)e$
Barnett&Smart	$Z+N(N-1)m$

Tabela 2: Časovna zahtevnost odpiranja kart

	Časovna zahtevnost vlečenja
Protokol miselnega pokra	$(N-1)Z+Ne$
Castella-Rocca	$(N-1)Z+(N+\frac{M}{2})e$
Barnett&Smart	$(N-1)Z+Ne+Nm$

Tabela 3: Časovna zahtevnost vlečenja kart

Iz zgornjih tabel lahko razberemo, da je naš protokol hitrejši od drugih protokolov tako v časovni zahtevnosti odpiranja kart kot tudi v časovni zahtevnosti vlečenja kart.

4 Uporaba protokola

Opisan protokol se lahko uporabi predvsem pri igrah s kartami. Ker pa se tudi igre kart se med seboj razlikujejo, jih ločimo glede na:

- število porabljenih kart na posamezno rundo,
  - naš protokol je časovno odličen za igre, kjer se uporablja veliko kart
- pomembnost, da so karte igralca drugim skrite (varnost protokola),
  - varnost je v našem protoklu zagotovljena, kot je podrobneje opisano v prejšnjem poglavju
- število potrebnih mešanj med trenutno rundo.

Zaradi naštetih lastnosti opisanega protokola je le-ta bolj prilagojen igram, kjer med igro uporabimo več (oz. kar vse) kart, ponovnega mešanja med igro pa ni. Igre, ki vsebujejo te lastnosti so Poker, Remi, Tarok, Most, ipd. Predvsem igra Poker je najbolj varna pri miselnem pokru, glede na to, da je edina možnost goljufanja medsebojna komunikacija po skritih kanalih. Gre za igro, kjer razkritje kart drugemu igralcu negativno vpliva na igro goljufa, ki informacijo podaja. Pri igri Tarok pa imamo problem predvsem s komunikacijo po zalednih sistemih. Informacija, kdo v roki drži "klicanega" kralja, bi pomenila ključ do zmage. Pravila igre Tarok so, da eden izmed 4 kraljev (klicani kralj) pove, katera dva igralca (izmed štirih) igrata skupaj. Če bi dva igralca po skritem kanalu prišla do ugotovitve, da igrata skupaj, bi oba spremenila strategijo odlaganja kart, ter si tako priigrala ključno prednost.
Kot smo povedali, je protokol časovno ugoden, ko uporabljamo več kart naenkrat, brez vmesnih mešanj podmnožice kart. V primerih, kjer se na posamezno rundo uporablja majhen odstotek kart, bi bilo smiselno vpeljati drugačen protokol mešanja. Primer takšne igre je Remi. Povedali smo sicer, da je naš protokol primeren za igro, ker ni vmesnih mešanj. Ker pa velik delež kart ne uporabimo, bi bilo bolje vpeljati način mešanja kart, kjer sproti (ko igralec vleče karto) generiramo naključno karto.

5 Zaključek

Za zaključek namenimo nekaj besed še prihodnosti in razvoju miselnega pokra.
Ena od možnosti za razvoj izvedbe miselnega pokra so vsekakor pametne kartice. V ta namen bi potrebovali v shemo vpeljati regulatorja, po možnosti državno institucijo, ki igralcem podeljuje spletno identiteto v obliki pametnih kartic. Pametno kartico je možno prevzeti le osebno, s čimer bi onemogočili ali vsaj močno otežili dostop do spletnega igralništva mladoletnim, znanim prestopnikom in odvisnikom od iger na srečo. Prav tako bi pametne kartice lahko prevzele tudi velik del računskega bremena, zato bodo v prihodnosti obravnavane kot ena bolj privlačnih rešitev (Trampuš, 2008) [5].
Varnost miselnega pokra pa bi lahko po mojem mnenju izboljšali tudi z vpeljavo umetne inteligence. Lahko

sklepamo, da bo v prihodnje umetna inteligenca ponujala možnost prepoznave govorice telesa in obraza. Z njeno pomočjo bi lahko med potekom igre poskrbeli, da avtomatsko zazna kretnje, ki so značilne za goljufanje in s tem prepozna nepoštene igralce.

V kriptografiji obstaja že kar nekaj različnih protokolov miselnega pokra. Vsak ima svoje prednosti ter slabosti. Naš protokol je varen, od drugih pa se razlikuje predvsem po hitrosti mešanja kart ob začetku igre. Dosegli smo dvakrat hitrejšo mešanje kart v primerjavi z Barnett & Smart in Castella-Roca protokoloma. Slabost našega protokola je mešanje podmnožice kart med samo igro.
Kot smo omenili že v uvodu, tudi ta protokol ni popoln. S trenutno znanimi kriptoalgoritmi nikomur še ni uspelo sestaviti protokola, ki bi bil 100% varen (brez možnosti medsebojnega sodelovanja), ob tem pa algoritmi ne bi bili časovno potratni. Miselni poker zato še vedno ostaja odprt problem. Ker pa protokol miselnega pokra temelji na izbiri splošnih kriptografskih shem in algoritmov, bo kakovost protokolov rasla skupaj z drugimi algoritmi na področju kriptografije. Čas bo tudi pokazal, ali bo miselni poker ostal le zanimiv teoretičen problem, ali pa bo postal eden temeljev večmiljardne industrije.

LITERATURA

[1] T. Wei in L. Wang, *A fast mental poker protocol*, Journal of Mathematical Cryptology, maj 2012, dostopno na https://www.degruyter.com/view/journals/jmc/6/1/article-p39.xml?language=en&tab_body=pdf-79694, prva objava : Januar 25, 2007.

[2] A. Shamir, R.L. Rivest, L. Adleman, D.A. Klarner,*Mental poker*, The Mathematical Gardner, Wadsworht international, 1981, dostopno na https://link.springer.com/chapter/10.1007%2F978-3-662-49896-5_12.

[3] J. Bootle, A. Cerulli, P. Chaidos, J. Groth, C. Petit, *Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting*, University of Oxford, 2016, dostopno na https://eprint.iacr.org/2016/263.pdf.

[4] M. Green, *Poker is hard, especially for cryptographers*, april 2012, dostopno na https://blog.cryptographyengineering.com/2012/04/02/poker-is-hard-especially-for/.

[5] M. Trampuš, *Miselni poker*, diplomska naloga na univezitetnem interdisciplinarnem študiju matematike in računalništva, 2008, dostopno na https://repozitorij.uni-lj.si/IzpisGradiva.php?id=24377&lang=slv&fbclid=IwAR0buIC_qmB5gwo1VVuKKFuDCaY9mMoCqvz9jHtLUG3vBXJlAW4U8KSONX8.

[6] P. Golle, *Dealing cards in poker games*, Palo Alto Research Center, 2005, dostopno na https://crypto.stanford.edu/~pgolle/papers/poker.pdf.

[7] Wikipedia, *Mental poker*, december 2019, dostopno na https://en.wikipedia.org/wiki/Mental_poker.

[8] Wikipedia, *Commitment scheme*, julij 2021, dostopno na https://en.wikipedia.org/wiki/Commitment_scheme#Coin_flipping.