Miselni poker

Seminarska naloga iz Kriptografije in teorije kodiranja 2

Mitja Trampuš

pomlad 2008

Povzetek

Kdo in kako naj meša karte, če želijo poker preko interneta igrati igralci, ki ne zaupajo niti drug drugemu niti tretjim osebam? Na naslednjih straneh najprej natančneje opišemo problem, nato v zgodovinskem pregledu izpostavimo najpogostejša matematična orodja ter pasti pri njegovem reševanju, zaključimo pa z razmeroma podrobnim opisom konkretne kriptografske sheme, ki nam omogoča igranje pokra na omenjeni način.

Kazalo

1 Motivacija **3**

2 Formalni opis problema **3**

3 Zgodovinski pregled **4**

3.1 Vpeljava problema in enostavna rešitev 4

3.2 Center zaupanja 6

3.3 K izpolnitvi Crépeaujevih zahtev 6

3.4 Sodobne sheme 7

4 Primer implementacije **7**

4.1 Osnovne operacije 7

4.1.1 Inicializacija 7

4.1.2 Mešanje kart 8

4.1.3 Vlečenje karte 10

4.1.4 Razkrivanje karte igralcem 11

4.1.5 Odmetavanje karte 12

4.2 Varnost 12

4.3 Učinovitost 13

5 Zaključek **13**

1 Motivacija

Z razmahom interneta se je pojavila tudi možnost spletnih partij pokra in drugih iger s kartami. Denarni promet na tem področju se meri v desetmestnih dolarskih številkah na leto. In kakor hitro igra vključuje denarne stave, je naravno, da pomislimo tudi na možnost goljufij. Igralci zato svojim soigralcem tipično ne zaupajo, še posebno na internetu, kjer so identitete močno zakrite. Le kako naj verjamemo anonimnemu soigralcu, ki nam preko spleta med igro virtualnega pokra zatrdi, da v rokah drži štiri ase? Navadno se takšne igre igrajo na nekem neodvisnem namenskem strežniku, ki na začetku igre razdeli karte in lahko zato takšne trditve igralcev potrdi ali ovrže. Pa vendar, kako naj bomo prepričani, da ni na primer eden od soigralcev kar lastnik strežnika in si lahko zato na strežniku ogleduje naše karte? Kljub takšnim utemeljenim pomislekom trenutno vse spletne poker hiše implicitno zahtevajo, naj igralci slepo verjamejo, da njihovi strežniki karte delijo pravično.

Kot rešitev tega problema so bile v zadnjih letih pod imenom "miselni poker" razvite praktično uporabne kriptografske rešitve, ki onemogočajo goljufanje vsem vpletenim v igri. Oglejmo si jih.

2 Formalni opis problema

Pojem miselnega ali mentalnega pokra ni povsem strogo definiran. Ozko gledano gre za problem varnega in poštenega igranja pokra med n igralci preko računalniškega omrežja. Pri tem ne želimo nobenemu igralcu izkazati večjega zaupanja ali dati večje pristojnosti kot preostalim.

Katere lastnosti igro opredelijo kot varno in pošteno, je 1985 prvič poskusil opisati Crépeau [6]:

a) **Odsotnost centra zaupanja** (Trusted Third Party, TTP). Ni dovolj, da so igralci enakovredni, tudi privilegiranega neigralca ne sme biti.

b) **Unikatnost kart.** Igralci morajo imeti možnost prepričati se, da nista npr. dva igralca dobila pikovega asa.

c) **Enakomerno naključno mešanje.** Pri mešanju kart naj ima vsaka možna permutacija enako verjetnost.

d) **Odkrivanje goljufij.** Verjetnost, da poljubna goljufija ostane neopažena, mora biti matematično majhna.

e) **Tajnost kart.** O kartah, ki jih igralec drži v rokah, ostali ne smejo dobiti niti bita informacije. Podobno velja za karte v kupčku.

f) **Tajnost strategije.** Igralci morajo biti zmožni dokazati svojo poštenost, ne da bi ob koncu igre razkrili svoje parametre kriptosistema. S tem bi namreč nujno razkrili tudi, katere karte so na koncu imeli v roki, s tem pa izničili "blef", pomembno komponento pokra.

g) **Minimalen vpliv zarot.** Če se nekaj igralcev zaroti proti ostalim in si med seboj namerno izmenjajo informacije o kartah in kriptosistemu, naj o kartah ostalih igralcev zvejo le toliko, kot če bi si pokazali le karte (namreč natančnejšo verjetnostno porazdelitev kart soigralcev). Ne smejo pa biti sposobni zlomiti ali načeti varnosti kriptosistema.

Te zahteve so se tekom časa dobro uveljavile in avtorji jih pri snovanju shem še vedno smatrajo za dobro referenco. Kljub temu je bilo do danes objavljenih presenetljivo malo kriptografskih shem, ki bi zadovoljile prav vsem zaželenim lastnostim z zgornjega seznama. Izkazalo se je namreč, da je takšno shemo precej težko razviti, še posebej, če želimo, da bo hkrati tudi računsko dovolj nezahtevna za uporabo v praksi.

Nekateri avtorji namesto ozkega osredotočanja na poker raje nekoliko ohlapneje govorijo o **miselnih igrah s kartami**, katerih predstavnik je seveda tudi miselni poker. Še več: poker se izkaže za eno izmed kompleksnejših iger, če ga želimo kriptografsko prirediti v "miselno" različico, torej za igranje preko omrežja. Tako se smatra, da je osredotočanje na poker dober korak k razvoju splošnega kriptografskega ogrodja za miselno igranje iger s kartami.

V čem se skriva kompleksnost miselnega pokra? Med partijo pokra so v vsakem trenutku lahko karte v vseh treh različnih stanjih vidnosti (v kupčku oz. vidna nikomur, v roki oz. vidna enemu igralcu, na mizi oz. vidna vsem). Poleg tega mora shema tako ali drugače omogočati razmeroma širok nabor operacij s kartami[1]:

- mešanje kart
- vlečenje karte iz kupčka
- umik karte iz obtoka
- prikaz izbrane karte vsem igralcem

Pod vplivom miselnega pokra se je razvilo tudi splošnejše področje **veččlanskega računanja** (Multiparty computation) [10], ki se ukvarja s temle problemom: Podatki $x_1, ..., x_n$ so razdeljeni med n oseb. Vse osebe poznajo tudi neko funkcijo $F(x_1, ..., x_n)$. Kako naj izračunajo vrednost funkcije, ne da bi katerikoli oseba morala svoj podatek x_i razkriti katerikoli drugi osebi?

3 Zgodovinski pregled

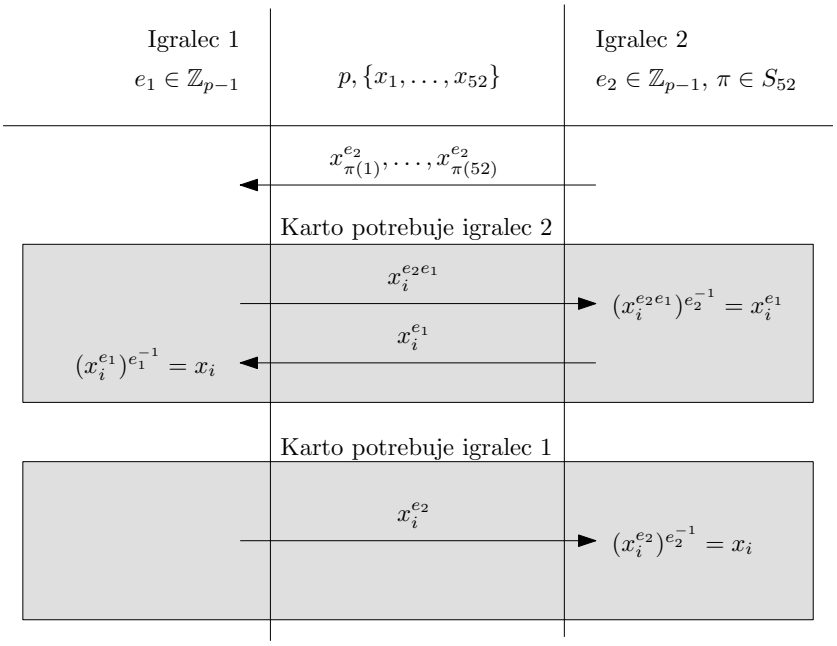
3.1 Vpeljava problema in enostavna rešitev

Problem miselnega pokra si je zamislila in opisala slavna trojica Shamir-Rivest-Adleman leta 1979 v članku "Mental poker". Njihov cilj ni bil zgraditi praktično uporabno shemo, temveč razmisliti, ali je taka shema sploh teoretično izvedljiva. Pokazali so, da brezpogojno varne sheme ni mogoče razviti, če pa se omejimo na računsko varnost, so rešitve možne.

Shema SRA

V istem članku so tudi že opisali nadvse preprosto shemo za igranje miselnega pokra za dva igralca, ki je računsko varna. Temelji na problemu diskretnega logaritma [9]. Ponazarja jo 3.1, nekoliko natančneje pa jo opišemo v sledečih alinejah.

[1] Ker so obstoječe sheme osredotočene na poker, so nekatere od naštetih operacij pogosto združene v eno obsežnejšo, ki pa jo je kriptografsko lažje implementirati.



Slika 1: Vrednosti nad zgornjo črto so vnaprej dogovorjene ali pa jih igralca določita samostojno.

1 **Predprirava.** Igralca se dogovorita za praštevilo p in 52 števil $\{x_1, ..., x_{52}\} \in \mathbb{Z}_p^*$, ki bodo predstavljala karte. Vse nadaljno računanje bo potekalo v $\mathbb{Z}_p^*$. Vsak od igralcev si izbere še svoje zasebno število, označimo ga e_1 oz. e_2, $e_1, e_2 \in \mathbb{Z}_{p-1}$.

2 **Mešanje kart.** Drugi igralec karte premeša z neko permutacijo π in nato vse karte zašifrira tako, da jih potencira s svojim tajnim številom e_2. Rezultat pošlje prvemu igralcu.

3 **Vlečenje/izbiranje karte.** Prvi igralec dobi $x_{\pi(1)}^{e_2}, ..., x_{\pi(52)}^{e_2}$, torej premešane in zašifrirane karte. Ker o njih ne ve ničesar, jih bo gotovo izbiral pošteno, naključno:

   (a) **Če karto potrebuje drugi igralec**, prvi igralec naključno izbere nek $i \in \{\pi(1), \ldots, \pi(52)\} = \{1, \ldots, 52\}$, izvleče karto $x_i^{e_2}$ in jo preda drugemu. Ta jo potencira na e_2^{-1} in dobi $x_i^{e_2 e_2^{-1}} = x_i$.

   (b) **Če karto potrebuje prvi igralec**, jo izvleče sam. Preden jo odda drugemu v odšifriranje, jo zakrije še s svojim ključem. Drugi igralec tako prejme $x_i^{e_2 e_1}$. Ker pozna svoj ključ e_2, lahko konstruira njegov inverz $e_2^{-1} \pmod{p-1}$ in s potenciranjem dobi $(x_i^{e_2 e_1})^{e_2^{-1}} = x_i^{e_1}$. Tega pošlje nazaj prvemu igralcu, ta pa od tu podobno kot prej drugi igralec rekonstruira x_i.

Shema je primerna kot zgled, ne pa tudi za praktično uporabo, saj ima več pomanjkljivosti. Prva, očitna, je omejitev na dva igralca[2].

Drugič, igralca morata ob koncu igre razkriti svoje ključe, če hočeta dokazati, da sta karte odšifrirala pošteno. S tem se izgubi tajnost strategije (f), kakršno smo po Crépeaujevem zgledu zahtevali v uvodnem poglavju.

[2]Poznejši avtorji so z razširitvijo sheme to omejitev odpravili

Tretjič, shema omogoča goljufanje: potenciranje števil x_i ohranja kvadratne ostanke [9]. Tudi o zašifrirani nasprotnikovi karti lahko tako igralec dobi vsaj en bit informacije.

3.2 Center zaupanja

Ko razmišljamo, kako bi implementirali miselni poker, je ena najpreprostejših in najbolj logičnih idej uvedba nekega poštenega razsodnika (center zaupanja, TTP), ki v igri ne bo udeležen. Če ga s sistemom javne kriptografije povežemo z vsemi igralci, lahko TTP opravi celotno mešanje, deljenje kart in preverjanje poštenosti igre.

Vendar pa zahteva (a) iz razdelka 2 prepovedujejo TTP. Ta ima namreč zaradi svoje privilegirane vloge popoln pregled nad igro in kartami igralcev. En sam igralec tako lahko dobi popolno informacijo o igri, čim podkupi TTP ali ga kontrolira kako drugače.

Omenili smo že, da je vse Crépeaujeve lastnosti v praksi težko doseči hkrati, če želimo, da bo shema učinkovita. Mnogo bolj praktično naravnanih avtorjev je zato uvedbo TTP videlo kot nujen kompromis, in še leta 2002 je bila predlagana shema s TTP.

Predlagane sheme seveda niso tako preproste kot zgoraj opisani trivialni primer, ko TTP nadzira prav vse. Z uporabo kriptografije poskušajo čim bolj zmanjšati njegove pristojnosti in omogočiti igralcem, da preverjajo njegovo poštenost.

Zmanjšanje pristojnosti TTP sheme tipično dosežejo tako, da igralci neodvisno določijo parametre njegovega delovanja (npr. izberejo vsak eno permutacijo), TTP pa te parametre skrivoma združi in se po njih ravna (npr. zmeša karte s kompozitumom permutacij igralcev). Shema omogoča, da se po končani igri igralci prepričajo, da je TTP res ravnal v skladu s poslanimi parametri.

Takšno preverjanje najpogosteje izvedemo z uporabo zaprisege bitov (bit commitment) [9]. A preverjamo lahko le poštenost v računskem smislu, ne moremo pa se izogniti na začetku opisanemu scenariju zarote, ko se eden od igralcev poveže s TTP.

3.3 K izpolnitvi Crépeaujevih zahtev

Vzporedno z rešitvami, ki uporabljajo TTP, so se razvijale tudi takšne brez njega. Ker pa avtorji še vedno niso znali hkrati doseči vseh želenih lastnosti miselnega pokra, so morali kompromise sklepati drugje. Največ takšnih rešitev zahteva, da igralci na koncu igre za dokaz poštenosti razkrijejo svoje parametre kriptosistema, s tem pa tudi svoje karte in strategijo.

Pogosto so bile sheme tudi neodporne na zarote skupin igralcev. Prvi je na zarote odporno shemo predstavil kar Crépeau v istem članku, v katerem je predstavil seznam zahtevanih lastnosti miselnega pokra.

Leto pozneje, 1986, je isti avtor svojo shemo dopolnil, da ni prisilila igralcev v razkritje strategij, in s tem predstavil prvo shemo, ki je zadoščala vsem njegovim zahtevam. Kasneje je to uspelo še nekaj avtorjem, vendar so bile vse sheme za praktično uporabo računsko prezahtevne. Leta 1994 je tako na primer mešanje kart za igro s tremi igralci na Sparcih trajalo osem ur.

3.4 Sodobne sheme

Prvo dovolj učinkovito shemo, ki je izpolnjevala vse varnostne pogoje, je leta 2003 opisal Španec Jordi Castellà-Roca. Nizko računsko zahtevnost je dosegel z uporabo homomorfnih šifrirnih funkcij [1]. Dve leti pozneje je predlagal še eno shemo z enakimi lastnostmi; ta je osnovana na dokazih brez razkritja znanja (zero-knowledge proof). Še istega leta je med želene lastnosti miselnega pokra dodal odpornost na izpad igralcev iz igre (bodisi namerno tik po izstopu iz igre bodisi zaradi prekinjene internetne povezave) in razširil svojo prejšnjo shemo, da je dobila tudi to lastnost. S tem je vpeljal in izpolnil novo zaželeno lastnost, vendar je pri tem shemo žal naredil neuporabno počasno [2].

Leta 2005 je Philippe Golle opazil, da vse obstoječe sheme na začetku igre rabijo veliko časa, da zmešajo vseh 52 kart, nato pa operacije stečejo hitro. To pomanjkljivost je odpravil v shemi [7], ki temelji na ElGamalovi enkripciji (enako kot mnoge prepočasne sheme), vendar "zmeša" le toliko kart, kot je nujno potrebno za trenutni krog. S tem se računsko delo porazdeli med več krogov igre (pri pokru štirje) in postane bolj obvladljivo in po zatrjevanju avtorja tudi uporabno. Edina slabost sheme je, da je razmeroma ozko osredotočena na poker. Za druge igre, kjer se karte odpira postopoma (npr. Blackjack ali v neki meri Enka), bi bila uporabna z manjšimi predelavami, za igre kot tarok pa sploh ne.

Leta 2006 je Castellà objavil še predlog [4] celovitega sistema za spletni poker, ki temelji na pametnih karticah. Te opravljajo vse kriptooperacije, potrebne med igro, hkrati pa je z njimi poskrbljeno tudi za nakazilo denarja, registracijo igralcev pri državnem regulatorju in podobno. S tem se članek dotakne tudi nematematičnih, a za problematiko igralništva družbeno pomembnih tem kot je preprečevanje iger na srečo mladoletnikom in rehabilitiranim odvisnikom.

Čeprav so najnovejše sheme varnejše in tudi že bistveno hitrejše od tistih izpred nekaj deset let, so kljub temu še vedno računsko tako zahtevne, da so uporabne le pogojno. V praksi danes zato še niso široko uveljavljene, implementirane in uporabljane; prevladujejo centralizirane sheme s TTP.

4 Primer implementacije

V nadaljevanju si bomo ogledali konkretno shemo za igranje mentalnega pokra, ki je razmeroma učinkovita, a kljub temu še obvladljivo kompleksna. Njena varnost sloni na odločitvenem Diffie-Hellmanovem problemu [9] ter na dokazih brez razkritja znanja [9]. Prvič je bila opisana leta 2005 v doktorski disertaciji Jordija Castellà-Roce; omenili smo jo že v prejšnjem poglavju.

4.1 Osnovne operacije

Igro pokra v mislih razbijemo na pet operacij: inicializacija, mešanje kart, vlečenje karte, razkrivanje karte soigralcem in odmetavanje karte. Vsaki od teh ustreza v naši shemi zaključen protokol.

4.1.1 Inicializacija

Predpostavimo, da imamo vzpostavljeno "oglasno desko" *(bulletin board)*, preko katere igralci izmenjujejo sporočila. Vsa komunikacija je javna in poteka preko te oglasne deske.

Prav tako predpostavimo, da so igralci dogovorjeni za vrednosti parametrov sheme:

- Veliko[3] praštevilo p oblike $p = 2q+1$, pri čemer je tudi q praštevilo. S tem postane problem diskretnega logaritma v $\mathbb{Z}_p^*$ odporen tudi na napad index caluclus [9];
- nekvadratni ostanek $\alpha \in \mathbb{Z}_p^*$, ki nam generira ciklično grupo $G \subset \mathbb{Z}_p^*$;
- varnostni parameter $s \in \mathbb{N}$ s priporočeno vrednostjo približno 10;
- število kart; v nadaljevanju bomo privzeli 52 kart in tega ne bomo označevali s spremenljivko.

Ko je tem predpostavkam zadoščeno, se igra začne s protokolom Inicializacija. Število igralcev pri tem označimo z n.

Protokol Inicializacija:

---

1 Vsak igralec P_i, $i \in \{1, \ldots, n\}$, izbere zasebni ključ a_i in objavi javni ključ $\beta_i = \alpha^{a_i}$.

2 Igralci skupaj izberejo naključno množico $X = \{x_1, \ldots, x_{52}\}$, $|X| = 52$, ki nam predstavlja čistopise igralnih kart. Za vsak $x_i \in X$ mora veljati $2 < x_i < q$, x_i je lih.

3 Igralci izračunajo $\beta = \alpha^{a_1 \cdots a_n}$ na naslednji način:

- Igralec P_1 objavi $\tilde{\beta}_1 = \alpha^{a_1}$
- Preostali igralci P_i za $i = 2..n$, drug za drugim izračunajo $\tilde{\beta}_i = (\tilde{\beta}_{i-1})^{a_i} = \alpha^{a_1 \cdots a_i}$.
- Ko izračun iz prejšnje alineje naredi še n-ti igralec, imamo $\beta = \tilde{\beta}_n$.

Edina občutljiva informacija v zgornjem protokolu – zasebni ključi a_i, $i \in \{1, \ldots, n\}$ – varnostno ni ogrožena, saj lahko a_i izračunamo le kot $a_i \log_{\tilde{\beta}_{i-1}} \tilde{\beta}_i$; za ta izračun pa bi morali rešiti problem diskretnega logaritma.

4.1.2 Mešanje kart

Da dosežemo čim večjo odpornost proti koalicijam zarotnikov, tudi takšnim velikosti $n-1$, karte premeša vsak od igralcev. Pri tem jih hkrati tudi zašifrira, da drugi igralci ne morejo ugotoviti uporabljene permutacije.

Označimo nepremešane karte z množico $C_0 = \{c_{0,1}, ..., c_{0,52}\}$. Dogovorili smo se, da nam karte predstavljajo števila x_i, in res zapišemo vsak $c_{0,i}$ kot par $(d_{0,i}, \alpha_{0,i})$, pri čemer je $d_{0,i} = \alpha^{x_i}$ in $\alpha_{0,i} = \beta$. Prvi element para bo skrival vrednost karte, drugega pa bomo uporabili za preverjanje poštenosti igralcev in kot pomoč pri odšifriranju prvega.

Protokol Mešanje:

Vsak igralec P_i:

[3] Dovolj veliko, da diskretni logaritem v $\mathbb{Z}_p^*$ ni izračunljiv v doglednem času.

1 Izračuna $(C_i, R_i, \pi_i) :=$MešanjeKorak(C_{i-1});
objavi C_i, preostanek rezultata pa zadrži zase

2 S protokolom MešanjeDokaz$(C_{i-1}, C_i, \pi_i, R_i)$ brez razkritja znanja dokaže poštenost mešanja

---

n-ti igralec tako kot zadnji naračuna C_n, kar je naš končni premešani kupček kart. Oglejmo si še posamezni korak mešanja, MešanjeKorak, na katerega se sklicuje zgornji protokol. V nekoliko drugačni obliki nam bo prišel prav tudi pozneje, zato mu dodamo še opcijska parametra R in π.

Postopek MešanjeKorak$(C, [R, \pi])$:

---

1 Če R in π nista podana:
   (a) Izberi naključno množico $R = \{r_1, ..., r_{52}\}$, kjer je vsak r_i lih in v mejah $2 < r_i < q$.
   (b) Izberi naključno permutacijo π nad 52 elementi

2 Za $j = 1..52$ izračunaj $c'_j = (d_j^{r_j}, \alpha_j^{r_j})$, kjer je $(d_j, \alpha_j) =: c_j$ j-ti element vhodne množice C.

3 Uporabi π nad pravkar naračunanimi c_j; rezultat je $C^* := \{c'_{\pi(1)}, ..., c'_{\pi(52)}\}$

4 Vrni (C^*, R, π)

Kot zadnji, a najpomembnejši gradnik mešanja kart opišimo protokol, s katerim lahko igralec dokaže, da je preslikavo $C_{i-1} \mapsto C_i$ res naredil z uporabo postopka MešanjeKorak, ne da bi pri tem razkril uporabljena R in π. Dokaz je verjetnosten, stopnjo zanesljivosti (ki seveda pride za ceno računske zahtevnosti) pa določa varnostni parameter s.

Protokol MešanjeDokaz(C, C^*, π, R):

---

1 Za $k = 1..s$ izračunaj $(C_k^*, R_k, \pi_k) :=$MešanjeKorak(C^*) in objavi C_k^*

2 Prepusti ostalim igralcem, da določijo s-bitni izziv $\{u_1, ..., u_s\}$

3 Za $k = 1..s$:
   (a) Če je bit $u_k = 1$:
      i. Razkrij R_k ter π_k
      ii. Ostali igralci preverijo, da MešanjeKorak res preslika $C^* \overset{R_k, \pi_k}{\longmapsto} C_k^*$
   (b) Če je bit $u_k = 0$:
      i. Izračunaj $\pi'_k := \pi_k \circ \pi$ in $R'_k := \{r'_{k,1}, ..., r'_{k,52}\}$, kjer je $r'_{k,i} := r_i \cdot r_{k,\pi(i)}$
      ii. Razkrij R'_k in π'_k
      iii. Ostali igralci preverijo, da MešanjeKorak res preslika $C \overset{R'_k, \pi'_k}{\longmapsto} C_k^*$

Pri tem nismo natančno opisali, kako preostali igralci skupaj določijo s-bitni izziv. Ena od možnosti je, da vsak igralec neodvisno pošlje svoje s bitno zaporedje, kot izziv pa uporabimo `xor` vseh poslanih zaporedij. Neodvisnost poslanih zaporedij posameznih igralcev lahko dosežemo z uporabo sheme za zaprisežene bite.

Pravilnost dokaza brez razkritja znanja. Prepričajmo se, da MEŠANJEDOKAZ res deluje. Oglejmo si k-to od s iteracij.

Če MEŠANJEKORAK preslika $C \overset{R,\pi}{\longmapsto} C^* \overset{R_k,\pi_k}{\longmapsto} C_k^*$, potem zaradi svojih lastnosti (uporabljena sta le permutacija in potenciranje) in načina, kako smo konstruirali R_k', π_k', preslika tudi $C \overset{R_k',\pi_k'}{\longmapsto} C_k^*$ – to pa je prav preslikava, ki jo preverjajo soigralci v koraku 3.b.iii.

Če torej igralec pošteno uporabi MEŠANJEKORAK in preslika $C \mapsto C^*$ ter $C^* \mapsto C_k^*$, bo test soigralcev uspel ne glede na vrednost u_k: Če je $u_k = 1$, bo korak 3.a.ii očitno uspešen. Če pa je $u_k = 0$, bo po prejšnjem odstavku uspel test iz koraka 3.b.iii.

Igralec lahko poskuša goljufati in izračuna C_k^* na pravilen način, nato pa vmesni rezultat C^* zavrže in soigralcem podtakne lažnega. V tem primeru bo test iz koraka 3.a.ii spodletel.

Drugi možni način goljufanja je, da igralec kar takoj nepravilno generira C^*, nato pa iz njega pravilno izpelje C_k^*. Vendar je v tem primeru C_k^* nepravilno generiran glede na C, zato bo goljufija opažena v koraku 3.b.iii.

Varnost mešanja. Da dokažemo, da so karte res varno premešane, bomo uporabili domnevo o odločitvenem Diffie-Hellmanovem problemu; to je odločitveni problem oblike $\log_{g_1} y_1 \overset{?}{=} \log_{g_2} y_2$. Domneva pravi, da je ta problem računsko enako neobvladljiv kot problem diskretnega logaritma.

Za začetek pokažimo, da za šifrirano karto $c_{n,i} \in C_n$ nihče ne more ugotoviti njenega čistopisa x niti s poskušanjem. Označimo $R_k =: \{r_{k,1}, ..., r_{k,52}\}$. Spomnimo se, da ima šifrirana karta obliko $c_{n,i} = (d_{n,i}, \alpha_{n,i}) = (\alpha^{x_i \cdot r_{1,i} \cdots r_{n,i}}, \beta^{r_{1,i} \cdots r_{n,i}})$. Če želimo za nek fiksen x_j preveriti, ali ustreza čistopisu, preverjamo $\log_\alpha d_{1,j} \overset{?}{=} x_i \cdot \log_\beta \alpha_{1,i}$. Če bi za ta problem imeli učinkovit algoritem A, bi lahko učinkovito rešili tudi odločitveni Diffie-Hellmanov problem, in sicer tako, da bi v A vstavili poljuben x ter preostale parametre nastavili na $\alpha := g_1$, $d_{n,i} := y_1^x$, $\beta := g_2$, $\alpha_{n,i} := y_2$. Prišli smo do protislovja, torej takšen algoritem v praksi ne obstaja.

Prepričati se moramo še, da igralci kart ne morejo slediti: noben igralec razen P_i ne sme biti sposoben ugotoviti, ali sta $c_{i-1,j} \in C_{i-1}$ in $c_{i,k} \in C_i$ ena in ista karta. Če gre res za isto karto, je $k = \pi_{i-1}(j)$ in je $c_{i,k}$ oblike $(d_{i,k}, \alpha_{i,k}) = ((d_{i-1,j})^{r_{i-1,j}}, (\alpha_{i-1,j})^{r_{i-1,j}})$. Da bi ugotovili $c_{i-1,j} \overset{?}{=} c_{i,k}$, moramo torej preveriti $\log_{d_{i-1,j}} d_{i,k} \overset{?}{=} \log_{\alpha_{i-1,j}} \alpha_{i,k}$. To pa je primer odločitvenega Diffie-Hellmanovega problema in zato ni učinkovito rešljiv.

4.1.3 Vlečenje karte

Denimo, da želi igralec P_u povleči novo karto. Lahko mu popolnoma zaupamo, da si bo karto izbral naključno (izbrati mora enega od elementov iz C_n, in o nobenem ne ve ničesar). Prav tako je ves čas jasno, katere zašifrirane karte so že bile izvlečene, zato tudi tu goljufanje ni mogoče. Naš protokol zato le poskrbi, da bo P_u izvlečeno karto lahko odšifriral.

Chaum-Pedersenov dokaz. Omenili smo že, da je problem $\log_{g_1} y_1 \overset{?}{=} \log_{g_2} y_2$ težek. Če pa nekdo ve, da je odgovor pritrdilen in celo pozna vrednost obeh logaritmov, lahko to dokaže s Chaum-Pedersenovim dokazom brez razkritja znanja [5]. Ker ga bomo v nadaljevanju potrebovali, si ga oglejmo. Vrednost obeh logaritmov označimo z x.

Protokol ChaumPedersen(g_1, y_1, g_2, y_2):

---

1 Dokazovalec izbere naključen s in objavi $s_1 := g_1^s$ ter $s_2 := g_2^s$.

2 Preverjevalec izbere izziv c in ga pošlje dokazovalcu.

3 Dokazovalec vrne $t := s + cx$.

4 Preverjevalec sprejme dokaz, če velja $g_1^t = s_1 y_1^c$ in $g_2^t = s_2 y_2^c$.

Ni se težko prepričati, da dokaz deluje. Dokazovalec ne izda nobene informacije o x, saj ga zaščiti z enkratnim ščitom s, ta pa je zaščiten z diskretnim logaritmom. Če dokazovalec res pozna x, se bodo enačbe v točki 4 izšle in dokaz bo sprejet. Če pa vrednosti x ne pozna, bi moral za generiranje veljavnega t rešiti diskretni logaritem.

Glavni protokol. Dokaz zdaj uporabimo v protokolu za vlečenje posamezne karte.

Protokol Vlečenje:

(Zaradi enostavnejšega zapisa brez škode za splošnost privzamemo, da karto vleče igralec P_n.)

1 P_n izbere tak indeks $i \in \{1, \ldots, 52\}$, da karta $c_{n,i} = (d_{n,i}, \alpha_{n,i}) \in C$ še ni bila uporabljena.

2 P_n objavi $e_0 := \alpha_n, i = \beta^{r_{1,i} \cdots r_{n,i}} = \alpha^{a_1 \cdots a_n \cdot r_{1,i} \cdots r_{n,i}}$.

3 Soigralci z e_0 odstranijo svoje privatne ključe $(a_1, ..., a_{n-1})$ na sledeči način:
Za $k = 1..(n-1)$:

(a) P_k izračuna in objavi $e_k := (e_{k-1})^{1/a_k}$

(b) P_k z vsakim od soigralcev uporabi ChaumPedersen$(\alpha, \beta_i, e_r, e_{r-1})$ in tako brez razkritja a_k dokaže, da je prejšnji korak izvedel korektno.

4 P_n odstrani še svoj privatni ključ: izračuna $e_n := (e_{n-1})^{1/a_n} = \alpha^{r_{1,i} \cdots r_{n,i}}$.

5 Z vstavljanjem vseh 52 možnih vrednosti za x igralec P_n najde čistopis karte, ki jo je povlekel: to je tisti x, ki zadosti enakosti $(e_n)^x = d_{n,i}$.

4.1.4 Razkrivanje karte igralcem

Karte $c_{n,i}$ ni težko pokazati soigralcem – njen čistopis preprosto objavimo na oglasni deski. Vendar pa jih moramo prepričati, da razkrivamo karto, ki smo jo nekoč res povlekli. To naredimo s sledečim kratkim protokolom.

Protokol Razkrivanje:

Tudi tu bomo zaradi enostavnejšega zapisa privzeli, da karto razkriva igralec P_n.

1 P_n objavi x ter $e_n = (e_{n-1})^{1/a_n} = \alpha^{r_{1,i} \cdots r_{n,i}}$.

2 P_n z vsakim od soigralcev uporabi ChaumPedersen$(e_n, e_{n-1}, \alpha, \beta_n)$ in tako brez razkritja a_n dokaže, da je prejšnji korak izvedel korektno.

3 Ostali igralci vsak zase preverijo, da x res zadosti enakost $(e_n)^x = d_{n,i}$.

Ker je P_n lahko e_n dobil le tako, da so mu ga nekoč pri vlečenju karte pomagali naračunati soigralci, s tem prepriča ostale igralce o svojem lastništvu karte.

4.1.5 Odmetavanje karte

Pri uporabljenem pristopu je ta operacija preprosta in ne potrebuje kriptografije. Ker igralci karte vlečejo z javnim izbiranjem elementov v množici šifriranih kart C_n, se za vsako šifrirano karto ve, kdo je njen lastnik. Ko igralec želi izločiti določeno karto, ne da bi razkril njen čistopis, mora zato le objaviti njen indeks v C_n.

4.2 Varnost

Oglejmo si še enkrat varnostne zahteve, ki smo jih našteli v 2. poglavju, in se prepričajmo, da jim opisana shema ustreza.

Odsotnost centra zaupanja. Vse operacije v vseh opisanih protokolih so popolnoma simetrične glede na vse udeležence, zato ni noben od igralcev privilegiran.

Unikatnost kart. Do podvajanja kart ali podobnih poskusov goljufanja lahko pride edino med mešanjem, saj se le tam spreminjajo opisi kart. Vendar pa je malo verjetno, da bo goljufanje ostalo neopaženo: vsak mešalec mora v protokolu MešanjeDokaz odgovoriti na s izzivov. Kot smo pokazali, lahko goljufiv igralec P_u na k-ti izziv pravilno odgovori le pri eni od dveh možnih vrednostih izziva u_k. Izziv sestavijo vsi igralci, zato že en sam pošten igralec zadošča, da je izziv res naključen in P_u ne more vnaprej sklepati na njegovo vrednost. Preostane mu slepo ugibanje, na katerega od izzivov naj se pripravi. Verjetnost, da bo pri tem uspešen, je $\frac{1}{2}$; ker pa je vseh izzivov s, kjer je s varnostni parameter, bo goljufijo neopaženo izpeljal z verjetnostjo samo $(\frac{1}{2})^s$.

Enakomerno naključno mešanje. Permutacija, s katero premešamo karte, je kompozitum permutacij posameznih igralcev. Že en sam pošten igralec, katerega permutacija je resnično naključna skrita pred soigralci, zadošča, da bodo karte premešane enakomerno naključno.

Odkrivanje goljufij. Kot smo pravkar pokazali, bo goljufanje med mešanjem kart odkrito z verjetnostjo $1 - (1/2)^s$. Goljufanje pri vlečenju ali razkrivanju karte pa je zaradi Chaum-Pedersenovega dokaza enako težko kot problem diskretnega logartima.

Tajnost kart. Če vsaj en od igralcev igra pošteno in svojo permutacijo π_i zadrži zase, ne more nihče ugotoviti, v katera karto iz $c_{n,i} \in C_n$ je bila zapermutirana neka nešifrirana karta iz C_0. Da pa iz $c_{n,i}$ ni mogoče odšifrirati tajnopisa, ne da bi poznali vse eksponente $r_{1,i}, ...r_{n,i}$ ali vse osebne ključe $a_1, ..., a_n$ smo pokazali že pri opisu protokola za mešanje.

Opozorimo še na označevanje kart: doslej predlagane sheme, ki temeljijo na potenciranju, pogosto razkrivajo en bit informacije o vsaki karti. Pri potenciranju se namreč ohranjajo kvadratni ostanki. V opisani shemi se temu že v začetku izognemo tako, da izberemo generator α, ki je nekvadratni ostanek, nato pa eksplicitno zahtevamo, da so vsi eksponenti, uporabljeni v igri, lihi. Da se njegovi soigralci držijo tega pravila, lahko preveri vsak igralec, saj je vsa komunikacija javna.

Tajnost strategije. Igralcem ob koncu igre ni treba razkriti svojih privatnih ključev ali kakršnihkoli drugih informacij, da bi dokazali svojo poštenost; ta se preverja že sproti. Potek igre ter karte, ki jih igralci obdržijo v roki, tako ostanejo tajne.

Minimalen vpliv zarot. Vsi izpeljani dokazi o varnosti kot predpostavko zahtevajo kvečjemu, da zlonamerni igralec za vsaj en u ne pozna eksponentov $r_{u,i}$, osebnega ključa a_u oziroma permutacije π_u. En sam pošten in nekompromitiran igralec P_u torej onesposobi zaroto preostalih $n-1$ igralcev.

4.3 Učinovitost

Kot pri veliki večini do zdaj predlaganih shem za mentalni poker je tudi pri naši mešanje kart časovno najbolj problematično. Čas, potreben za premešanje kart, je odvisen od števila igralcev, varnostnega parametra s in velikosti praštevilskega obsega p.

Čeprav shema ni bila nikoli implementirana, je avtor preštel število potenciranj in množenj, potrebnih v protokolu MešanjeKorak, nato pa eksperimentalno določil čas, potreben za eno potenciranje oziroma množenje. Tako je ugotovil, da bi na danes nekoliko starejših solidnih računalnikih (ThinkPad T41, Centrino 1.5GHz) mešanje trajalo približno 18 sekund na igralca, če uporabimo precej skromne varnostne parametre: 256-biten p in $s = 5$. Če varnost povečamo in postavimo $s = 15$ ter izberemo 512-biten p, časovna zahtevnost mešanja naraste na 312 sekund na igralca.

V primerjavi s starejšimi shemami je to opazen napredek, vendar hkrati s tem očitno še ne moremo biti dokončno zadovoljni.

5 Zaključek

Problem mentalnega pokra je, čeprav zanimiv tudi z izključno teoretičnega vidika, doživel renesanso z razmahom internetnega igralništva. Napredek v zadnjih letih je bil zato razmeroma hiter, in tako počasi prihajamo do shem, ki bi lahko zaživele tudi v praksi. Pravkar opisana je precej na meji: če predpostavimo, da so uporabniki pripravljeni čakati kakšno minuto, preden se posamezna igra začne, in če se zadovoljimo z zmerno varnostjo, bi bil protokol morda celo uporaben. A velikim internetnim poker hišam je jasno, da se igralci raje (morda nevede) zanesejo na poštenost in ime igralnice, kakor da bi morali dolgo čakati na vsako igro in s tem pridobili težko razumljive jim varnostne garancije. Poleg tega je hišam v interesu, da lahko vsako igro popolnoma nadzorujejo, saj tako dobijo vpogled v strategije in miselnost igralcev.

Na srečo obstajata še vsaj dve shemi, učinkovitejši od opisane. Prva je v razdelku 3.4 že omenjena Golle-ova [7], ki pa je razmeroma ozko specializirana za poker. V primerjavi z našo shemo na podlagi teoretičnih izračunov obeh avtorjev (nobena od shem ni bila zares implementirana –

stalna težava miselnega poka) lahko pričakujemo, da ta shema pri petih igralcih zahteva približno desetkrat manj operacij. Zasluge za drugo učinkovito shemo [1] gredo avtorju naše sheme. Podatkov o računski zahtevnosti ali hitrosti sicer ni, vendar Castellà v [3] zatrdi, da je shema patentirana, prodana podjetju *Scytl Online World Security, S.A* in tudi implementirana. Implementorji naj bi shemo opisali kot "časovno praktično uporabno".

Ta shema je torej najbrž trenutno najbolj aktualna, a žal nikakor ne tako nazorna in razumljiva kot ta, ki smo jo opisali: inicializacija in vlečenje karte na primer zahtevata vsaka po 15 korakov. Takšna kompleksnost shemo gotovo dela manj privlačno za uporabo v praksi in pušča še veliko odprtega prostora za napredek in izboljšave. Te pa so možne in potrebne ne le na področju kompleksnosti, temveč tudi hitrosti.

Čez kakih deset let, ko bo kriptografija miselnega kvartopirstva, upajmo, napredovala, pohitrili pa se bodo tudi računalniki, najverjetneje lahko pričakujemo, da bodo poštene in varne sheme končno zaživele in postale široko razširjene tudi v praksi.

Literatura

Za dober pregled nad podrocjem miselnega pokra priporočam zelo prikladno Stamerjevo bibliografijo [8], ki jo avtor redno obnavlja in ki našteva vse relevantne članke s področja skupaj z njihovimi povzetki.
Castellà-Roca v svoji disertaciji [3] med drugim na pregleden in konsistenten način temeljito obdela večino shem, znanih do približno leta 2004.

[1] Jordi Castellà Roca in drugi, "Practical Mental Poker Without a TTP Based on Homomorphic Encryption," v zborniku *Progress in Cryptology (INDOCRYPT 2003), 4th International Conference on Cryptology*, New Delhi, India, december 2003, strani 280–294

[2] Jordi Castellà-Roca, Francesc Sebé, Josep Domingo-Ferrer, "Dropout-Tolerant TTP-Free Mental Poker," v zborniku *Trust, Privacy and Security in Digital Business: Second International Conference (TrustBus 2005)*, Copenhagen, Denmark, avgust 2005, strani 30–40

[3] Jordi Castellà Roca, *Contributions to Mental Poker*, doktorska disertacija, Universitat Autònoma de Barcelona, 2005

[4] Jordi Castellà-Roca, Josep Domingo-Ferrer, Francesc Sebé, "Smart-Card Based Mental Poker," v zborniku *Smart Card Research and Advanced Applications, 7th IFIP WG 8.8/11.2 International Conference (CARDIS 2006)*, Tarragona, Spain, april 2006

[5] David Chaum, Torben Pryds Pedersen, "Wallet Databases with Observers (Extended Abstract)," v zborniku *Advances in Cryptology - CRYPTO'92 Proceedings*, Santa Barbara, California, USA, avgust 1992, strani 89–105

[6] Claude Crépeau, "A Secure Poker Protocol that Minimizes the Effect of Player Coalitions," v zborniku *Advances in Cryptology - CRYPTO'85 Proceedings*, Santa Barbara, California, USA, avgust 1985, strani 73–86

[7] Phillippe Golle, "Dealing Cards in Poker Games," v zborniku *International Symposium on Information Technology: Coding and Computing (ITCC 2005), Volume 1*, Las Vegas, Nevada, USA, april 2005 strani 506–511

[8] Heiko Stamer, *Bibliography on Mental Poker*, 2007

[9] Douglas R. Stinson, *Cryptography: Theory and Practice*, tretja izdaja, CRC Press, 1995

[10] Andrew Chi-Chih Yao, "Protocols for secure computations", v zborniku *Proceedings of the twenty-third annual IEEE Symposium on Foundations of Computer Science*, Chicago, Illinois, USA, november 1982, strani 160–164.