Kártyajátékok kriptográfiájának vizsgálata és egy kártyajáték kriptográfiai megvalósítása

Diplomamunka

Írta: Török Sándor

Alkalmazott matematikus szak

Témavezető:

Gonda János, egyetemi docens

Komputeralgebra Tanszék

Eötvös Loránd Tudományegyetem, Informatikai Kar

Eötvös Loránd Tudományegyetem

Természettudományi Kar

2009

Előszó

Ezúton is szeretném megköszönni témavezetőmnek, Gonda Jánosnak e számomra igazán kedves téma felvetését, és építő észrevételeit közös munkánk során.
Hálával és köszönettel tartozom még családomnak: e dolgozat megírásához támogatásukra és türelmükre messzemenőkig szükségem volt.

Tartalomjegyzék

1. fejezet

Bevezetés

1.1. Motiváció

A kártyajátékok mindig is erősen hatottak a matematikára és a számítástechnikára. A kutatókat foglalkoztatta a véletlen struktúra megértése, a bennük rejlő kombinatorika és valószínűségek. Ma már nem csak a játékok elemzése, hanem számítógépes szimulációjuk is tudományos érdeklődést vált ki.

Napjainkban egyre növekszik az interneten online játszható kártyajátékok népszerűsége, az ebből származó pénzforgalom is egyre jelentősebb. A pénzüket kockáztató játékosok jogosan várják el a számítógépes kártyajáték szimulációkkal szemben, hogy azok garantálják a valódi játék feltételeit a küzdelem tisztasága érdekében.

Ezen elvárásoknak a legtöbb ma működő internetes online kártyajáték-szimuláció nem felel meg. Elsősorban azért, mert a legtöbb ilyen rendszerben a lejátszó felek közötti kommunikáció egy megbízható félként kezelt játékszerveren keresztül történik, ám felmerül a kérdés, hogy lehetséges-e egyáltalán a megbízhatóság mögé elégséges garanciákat felsorakoztatni.

A kártyajátékok megbízható fél nélküli implementációjának problémája a szakirodalomban a "Mental Card Games" vagy az e téren legtöbb figyelmet kapott kártyajáték neve után "Mental Poker" nevet viseli. A következőkben a tarokk kártyajátékra adunk ilyen jellegű megvalósítást.

1.2. Célkitűzések

A megbízható fél nélküli implementációval szemben még az alábbi követelményeket támasztjuk:

- **Kártyák egyedisége:** Biztosított, hogy a protokoll során előforduló kártyatípusok megegyeznek a valódi játék kártyatípusaival. A játékosok ellenőrizhetik, hogy minden kártyatípus pontosan egyszer fordul elő.

- **Kártyák véletlenszerűsége, egyenletes eloszlás szerint:** Az osztás során kiosztott kártyák egyenletes eloszlásból kell, hogy származzanak. Az egyes játékosok kiosztott lapjainak típusa az összes játékos döntéseinek függvénye.

- **Csalás észrevétele nagy valószínűséggel:** A protokoll észre kell, hogy vegye a csalási kísérleteket.
  Megjegyzés: Ezen a ponton a "Mental Poker" a szabályok betartásának azonnali ellenőrzésével biztonságosabb lehet, mint egy valódi játék.

- **Kártyatípusok bizalmas kezelése:** Ha a játék egy adott helyzetében bizonyos játékosok számára egy kártyának csak a hátoldala lenne látható a valódi játékban, akkor a kártya típusáról az ő számukra semmilyen információ nem szivároghat ki. Egy kártya húzása esetén a többi játékos semmilyen információt nem tudhat meg a kártya típusáról.

- **Titkos szövetségek minimális hatása:** Előfordulhat, hogy a játékosok egy része szövetségbe tömörülve titkos csatornán kommunikál a többi játékos ellen. Ebben az esetben egy nem csaló játékos kártyáiról nem szivároghat ki több információ, mint amennyit a titkos szövetség tagjai az egymásnak átadott információkból ki tudnak következtetni.
  Megjegyzés: Ezen a ponton a "Mental Poker" nem tudja egy valódi játék biztonságát garantálni. Eszközeinkkel nem ellenőrizhető, hogy a résztvevő felek egy csoportja kommunikál-e egymással egy titkos, a játék protokolljai által nem használt csatornán, de természetesen egy titkos koalíció még a fentiek figyelembevételével is a játék kimenetele szempontjából döntő, igazságtalan előnyhöz juttathatja a koalíció résztvevőit.

1.3. A dolgozat szerkezete

A 2. fejezetben bemutatjuk a feladat megoldásához használt kriptográfiai eszközöket.

A 3. fejezetben vázoljuk a kártyajátékok kriptográfiai modelljét, és bemutatjuk az elkövetkező tarokk implementáció fontosabb építőelemeit. A fentebb ismertetett célkitűzéseinkből néhánynak a teljesítése már itt megjelenik, ezt a megfelelő helyeken a célkitűzés nevére való hivatkozással jelezzük.

A 4. fejezetben megadjuk a tarokk implementálációját a protokollok algoritmusain és leírásán keresztül. Itt kerülnek sorra a 3. fejezetben még nem hivatkozott, további célkitűzéseink.

Az 5. fejezetben igazoljuk, hogy a 4. fejezet protokolljaival a feladatot megoldottuk.

A 6. fejezetben betekintését nyújtunk a szakirodalomba, elhelyezve dolgozatunkat a szakterület eredményei között.

A 7. fejezet függelék, egy tarokk szabályismertető.

2. fejezet

Kriptográfiai háttér

2.1. Az ElGamal nyilvános kulcsú rejtjelező algoritmusai és homomorf tulajdonsága

Az alábbiakban bemutatjuk, hogy két résztvevő fél közötti kommunikáció titkosításához hogyan használható fel az ElGamal rejtjelező rendszer. Első lépésként megállapodnak egy biztonságos G ciklikus, q rendű, multiplikatív csoportban, melynek g egy generátoreleme. A biztonság feltételeit később elemezzük. Természetesen ezen paraméterek nyilvánosak. Vezessük be az alábbi jelöléseket:

- üzenettér: $\mathcal{M} = G$
- kódtér: $\mathcal{C} = G \times G$
- véletlen elemek tere: $\mathcal{R} = \mathbb{Z}_q$

Az alábbi algoritmussal mindkét résztvevő fél létrehozza saját nyilvános és titkos kulcsát.

2.1.1. Kulcsok létrehozása

1. A résztvevő választ egy titkos $x \in \mathbb{Z}_q$ elemet
2. A résztvevő kiszámolja $h = g^x$-et
3. A résztvevő nyilvános kulcsa: (G, q, g, h), ezt közzéteszi; a résztvevő titkos kulcsa: x, ezt titokban tartja

A rejtjelező egy, a fejtőnek küldött $m \in \mathcal{M}$ elrejtéséhez a fejtő (G, q, g, h) nyilvános kulcsát használja fel.

2.1.2. Rejtés: $E : \mathcal{M} \times \mathcal{R} \longrightarrow \mathcal{C}$

1. A rejtjelező választ egy véletlen $y \in \mathcal{R}$ elemet
2. A rejtjelező kiszámolja $c_1 = g^y$-t és $c_2 = mh^y$-t
3. A rejtjelező elküldi a $(c_1, c_2) \in \mathcal{C}$ kódot a fejtőnek

A fejtő egy neki küldött $(c_1, c_2) \in \mathcal{C}$ rejtett üzenetet a titkos kulcsa, x segítségével az alábbiak szerint fejt meg.

2.1.3. Fejtés: $D : \mathcal{C} \longrightarrow \mathcal{M}$

1. A fejtő kiszámítja c_2/c_1^x-et, ennek eredménye éppen a megfejtett üzenet

A fejtés igazolása: $c_2/c_1^x = mh^y/g^{xy} = mg^{xy}/g^{xy} = m$

2.1.4. Homomorf tulajdonság

Az ElGamal rejtjelező rejtés operációja csoport-homomorfizmus az üzenettér és a kódtér között:

$$E(m_1, r_1) \cdot E(m_2, r_2) = (g^{r_1}, mh^{r_1}) \cdot (g^{r_2}, mh^{r_2}) =$$

$$= (g^{r_1+r_2}, (m_1 m_2)h^{r_1+r_2}) = E(m_1 \cdot m_2, r_1 + r_2)$$

Az $m_1 = m, \quad m_2 = 1$ speciális esetben:

$$E(m, r_1) \cdot E(1, r_2) = E(m, r_1 + r_2)$$

Így $m \in \mathcal{M}$ egy új rejtését kaptuk. Ez lehetőséget teremt a rejtési operáció kódtérre való következő természetes kiterjesztésére. Legyen $c \in \mathcal{C}$. Rendeljük ehhez hozzá a kódtér egy másik elemét az alábbi algoritmussal:

2.1.5. Újrarejtés a kódtéren: $E^{'} : \mathcal{C} \times \mathcal{R} \longrightarrow \mathcal{C}$

1. A rejtjelező választ egy véletlen $r \in \mathcal{R}$ elemet
2. A rejtjelező kiszámolja $c_1^{'} = c_1 g^r$-et és $c_2^{'} = c_2 h^r$-et
3. A rejtjelező elküldi a $(c_1^{'}, c_2^{'}) \in \mathcal{C}$ új kódot a fejtőnek

Az algoritmus értelmében

$$E^{'}(c, r) = c \cdot E(1, r)$$

Ekkor $c = E(m, r_1)$ és $r = r_2$ mellett

$$E^{'}(E(m, r_1), r_2) = E(m, r_1) \cdot E(1, r_2) = E(m, r_1 + r_2)$$

Tehát a homomorf tulajdonság következménye, hogy az újrarejtés operációval valóban az őskép üzenet egy új rejtését kapjuk. Ez azt jelenti, hogy egy üzenet újrarejtéséhez nem kell ismernünk az üzenetet magát. Az ElGamal rejtjelezőnek ez a tulajdonsága a továbbiakban nagyon hasznos lesz számunkra.

2.2. Az ElGamal rejtjelező biztonsága

2.2.1. Szemantikai biztonság (ss biztonság)

Shannon ideális rejtjelezője esetén, a rejtjeles szöveg ismeretében a nyílt szövegre vonatkozóan tetszőleges számítási kapacitás mellett sem tudunk meg a priori ismereteinknél több információt. Ennek a fogalomnak erőforrás-megszorítás melletti megfelelője a szemantikai biztonság fogalma.

Vezessük be a $g : \mathcal{M} \to \{0,1\}^*$ részinformáció leképezést. Például $g(m) = 1$, $m \in \{0,1\}^n$, ha az üzenetben "111" részsorozat előfordul. Kisorsolunk egy $m \in \mathcal{M}$-et, a támadó által is ismert eloszlás szerint. Szemantikai biztonság fennállása esetén, a támadó semmilyen g részinformációs függvény esetén sem tudja pontosabban becsülni $g(m)$ értékét $c = E(m)$ ismeretében, mint c ismerete nélkül. Formálisan:

Definíció: Egy nyilvános kulcsú rejtjelező $(t(n), \epsilon(n))$-szemantikailag biztonságos, ha nyílt üzenetek tetszőleges X eloszlása, $\forall g$ részinformációs függvény és $\forall t(n)$ erőforrás-korlátú hatékony Z támadó algoritmus esetén $\exists$ azonos erőforrás-korlátú

hatékony Z' támadó algoritmus, hogy

$$Pr_{m \leftarrow X}\{Z(E(m)) = g(m)\} - Pr_{m \leftarrow X}\{Z' = g(m)\} \leq \epsilon(n)$$

A Z és Z' algoritmusok mögött zárójelben azok inputja áll. Z' neve szimulációs algoritmus.

2.2.2. Üzenet-megkülönböztethetetlenség biztonság választott nyílt szövegű támadással szemben (ind-cpa biztonság)

Egy nyilvános kulcsú rejtjelezés üzenet-megkülönböztető választott nyílt szövegű támadással szemben biztonságos, ha a támadó nem tud megadni egy olyan üzenetpárt, amelyből, ha visszakapja az egyik, véletlenszerűen kiválasztott üzenet rejtjelezettjét, akkor nem elhanyagolható valószínűséggel meg tudja állapítani, hogy az melyik üzenethez tartozott.

Definíció: Egy nyilvános kulcsú rejtjelező üzenet-megkülönböztető támadással szemben $(t(n), \epsilon(n))$-biztonságú, ha $\forall m_0, m_1 \in \{0,1\}^n$ üzenetpár és $\forall t(n)$ erőforráskorlátú hatékony Z támadó algoritmus esetén

$$Pr_{b \in \{0,1\}}\{Z(m_0, m_1, E(m_b)) = b\} \leq 1/2 + \epsilon(n)$$

2.2.3. Kapcsolat a biztonság definíciók között

Tétel: ss biztonság $\Rightarrow$ ind-cpa biztonság

Bizonyítás: Az ss biztonság definícióban legyen az X üzeneteloszlás egyenletes az $\{m_0, m_1\}$ halmazon, és legyen $g(m_0) = 0, g(m_1) = 1$. Ekkor egy Z ss-támadó egyben ind-támadó is. Az ss biztonság definíciója szerint ugyanis

$$Pr_{b \in \{0,1\}}\{Z(m_0, m_1, E(m_b)) = b\} \leq Pr_{b \in \{0,1\}}\{Z' = b\} + \epsilon(n) = 1/2 + \epsilon(n)$$

Tétel: ind-cpa biztonság $\Rightarrow$ ss biztonság

Bizonyítás: Indirekt tegyük fel, hogy a Z ss támadó $(t(n), \epsilon(n))$-töri a rejtjelezőt, azaz $\forall Z'$ szimulációs algoritmus esetén

$$Pr_{m \leftarrow X}\{Z(E(m)) = g(m)\} - Pr_{m \leftarrow X}\{Z' = g(m)\} > \epsilon(n)$$

Megmutatjuk, hogy Z használható ind-cpa támadásra. A kapocs a kétféle biztonságdefiníció között az az észrevétel, hogy az ss biztonság definíciójabeli Z' szimulációs

algoritmusra fennáll a $Z' = Z'(E(0))$ egyenlőség, hiszen $E(0)$ előállítható kizárólag a nyilvános kulcs ismeretében. Mivel a fenti egyenlőtlenség $\forall Z'$ szimulációs algoritmus esetén fennáll, így akkor is fennáll, ha Z'-t Z-vel helyettesítjük:

$$Pr_{m \leftarrow X}\{Z(E(m)) = g(m)\} - Pr_{m \leftarrow X}\{Z(E(0)) = g(m)\} > \epsilon(n)$$

Azaz:

$$\sum_m Pr\{m\} \left(Pr\{Z(E(m)) = g(m)\} - Pr\{Z(E(0)) = g(m)\}\right) > \epsilon(n)$$

Innen a skatulya-elv alapján létezik pozitív valószínűségű m^* üzenet, hogy

$$Pr\{Z(E(m^*)) = g(m^*)\} - Pr\{Z(E(0)) = g(m^*)\} > \epsilon(n)$$

Definiáljuk a Z^* támadó algoritmust a következőképpen:

Algoritmus:

1. Z^* inputja $(m_0 = 0, m_1 = m^*, E(m_b))$
2. Z^* meghívja Z algoritmust $E(m_b)$ inputtal
3. Z^* algoritmus outputja 1, ha Z outputja $g(m^*)$, egyébként Z^* outputja 0.

De ekkor a Z^* ind-cpa támadó $\epsilon(n)/2$-nél nagyobb sikervalószínűségű lenne, mert:

$$Pr_{b \in \{0,1\}}\{Z^*(m_0, m_1, E(m_b)) = b\} =$$

$$= 1/2 \left(Pr\{Z(E(m^*)) = g(m^*)\} + 1 - Pr\{Z(E(0)) = g(m^*)\}\right) >$$

$$> 1/2 + \epsilon(n)/2$$

2.2.4. Diffie-Hellmann eldöntési probléma (DDH)

Legyen $G = \langle g \rangle$ egy q rendű ciklikus csoport. Adott (g^x, g^y, g^z) hármas esetén el kell dönteni, hogy a kitevők között fennáll-e a $z = xy \bmod q$ összefüggés. Egy q prím Sophie-Germain prím, ha $p = 2q + 1$ is prím. A DDH feltevés szerint, ha q elég nagy Sophie-Germain prím, és G a mod p kvadratikus maradékok csoportja, akkor G-ben a DDH probléma megoldása nehéz.

2.2.5. ElGamal biztonsága

Állítás: Tegyük fel, hogy $G = \langle g \rangle$-ben nehéz a DDH probléma. Ekkor G-ben az ElGamal rejtjelező ind-cpa biztonságú.

Bizonyítás: A DDH problémára való redukcióval végezhető. Legyen Z egy támadó, amely sikeresen töri az ElGamal rejtjelezőt. Konstruáljunk egy Z' támadót, amely "töri" a DDH problémát a következőképpen:

Algoritmus:

1. Z' támadó Z támadónak g^x csoportelemet adja, mint nyilvános kulcsot.
2. Z előállít egy m_0, m_1 üzenetpárt.
3. Z' kisorsol egy b bitet, és Z-nek $(g^y, g^z m_b)$ rejtjelezett üzenetet küldi.
4. Ha Z outputja megegyezik b, akkor Z' outputja 1, azaz Z' döntése az, hogy (g^x, g^y, g^z) egy DDH-hármas, egyébként Z' outputja 0.

Következmény: Tegyük fel, hogy $G = \langle g \rangle$-ben nehéz a DDH probléma. Ekkor G-ben az ElGamal rejtjelező szemantikailag biztonságos.

2.3. Az ElGamal n-ből n küszöb nyilvános kulcsú rejtjelező

Ez az ElGamal rejtjelező olyan n résztvevős változata, ahol egy rejtjelezett üzenet fejtéséhez mind az n résztvevő közreműködése szükséges, bármely $n-1$ résztvevő együtt semmit nem tudhat meg az eredeti üzenetről.

Első lépésként a résztvevők itt is megállapodnak egy biztonságos G ciklikus, q rendű, multiplikatív csoportban, melynek g egy generátoreleme. Ezek a paraméterek nyilvánosak, és belátható, hogy ugyanolyan feltételek mellett biztonságosak, mint a két résztvevős esetben. $\mathcal{M}$, $\mathcal{C}$, $\mathcal{R}$ jelentsék ugyanazt, mint fentebb.

2.3.1. Kulcsok létrehozása

Az alábbi protokoll során a résztvevő felek generálnak egy közös h nyilvános kulcsot. Az ehhez ismeretlen x titkos kulcs szét van osztva az x_i részekben.

1. Minden résztvevő választ véletlenül egy titkos $x_i \in \mathbb{Z}_q$ elemet

2. Minden résztvevő kiszámolja $h_i = g^{x_i}$-t

3. A közös nyilvános kulcs: $h = \prod_{i=1}^{n} h_i = g^x$, ahol $x = \sum_{i=1}^{n} x_i$

A következő algoritmus segítségével a közös h nyilvános kulcs felhasználásával egy $m \in \mathcal{M}$ elrejtését végzi egy résztvevő fél (a rejtjelező). Ez teljesen hasonló a két résztvevős ElGamal rejtjelezéshez.

2.3.2. Rejtés: $E : \mathcal{M} \times \mathcal{R} \longrightarrow \mathcal{C}$

1. A rejtjelező választ egy véletlen $r \in \mathcal{R}$ elemet

2. A rejtjelező kiszámolja $c_1 = g^r$-t és $c_2 = mh^r$-t

3. A rejtett üzenet $(c_1, c_2) \in \mathcal{C}$

Az alábbi protokoll segítségével a $(c_1, c_2) \in \mathcal{C}$ rejtett üzenetet megfejti egy résztvevő fél (a fejtő).

2.3.3. Fejtés: $D : \mathcal{C} \longrightarrow \mathcal{M}$

1. A fejtőnek minden i résztvevő elküldi $c_1^{x_i}$ fejtési információt

2. A fejtő kiszámítja $c_2 / \prod_{i=1}^{n} c_1^{x_i}$-t, ennek eredménye éppen a megfejtett üzenet

A két résztvevős ElGamal rejtjelezőnél látottak miatt a rejtjelezés homomorf tulajdonsága itt is fennáll, ezért itt is értelmezhetjük az újrarejtést. Továbbá a fentebb tárgyalt, őskép üzenettel kapcsolatos következtetések is fennállnak.

2.3.4. Újrarejtés a kódtéren: $E' : \mathcal{C} \times \mathcal{R} \longrightarrow \mathcal{C}$

1. A rejtjelező választ egy véletlen $r \in \mathcal{R}$ elemet

2. A rejtjelező kiszámolja $c_1' = c_1 g^r$-et és $c_2' = c_2 h^r$-et

3. Az új kód $(c_1', c_2') \in \mathcal{C}$

2.4. Nullaismeretű (zero-knowledge) bizonyítás

A nullaismeretű bizonyítás vagy nullaismeretű protokoll egy olyan interaktív eljárás, melynek során az egyik résztvevő, az igazoló fél úgy bizonyítja be egy állítást fennállását, hogy az állítás fennállásának tényén kívül az állítás tartalmáról semmilyen információt nem oszt meg a másik résztvevővel, az ellenőrző féllel.
Egy nullaismeretű bizonyítás a következő három tulajdonságot teljesíti:

1. **Teljesség:** Ha az állítás igaz, akkor erről a tényről egy becsületes igazoló fél meggyőz egy becsületes ellenőrző felet

2. **Helyesség:** Ha az állítás hamis, akkor egy csaló igazoló fél csak kis valószínűséggel tud az ellenkezőjéről meggyőzni egy becsületes ellenőrző felet.

3. **Nullaismeretű tulajdonság:** Ha az állítás igaz, akkor e tényen kívül egy csaló ellenőrző fél sem tud meg semmit az állításról.

A nullaismeretű bizonyítás matematikai értelemben nem tekinthető bizonyításnak, mert a 2. pont értelmében mindig van egy kis valószínűség, amellyel egy csaló igazoló fél meg tudja győzni a becsületes ellenőrző felet egy hamis állítás igazságáról. De ez a valószínűség az alkalmazásokban hatékonyan csökkenthető elhanyagolható mértékűre.
Az egyik legelbűvölőbb alkalmazási lehetősége a nullaismeretű bizonyításoknak egy más protokollba való beépítésükkel a becsületes (a protokoll szabályainak megfelelő) viselkedés kikényszerítése, a titoktartás megsértése nélkül. Ez nagy vonalakban úgy valósítható meg, hogy a protokollban előírjuk a résztvevő félnek, hogy nullaismeretű bizonyítással igazolja a protokoll egyéb lépéseinek becsületes végrehajtását. Hiszen egyrészt a helyesség miatt érvényes igazolást csak becsületes fél adhat, másrészt a nullaismeretű tulajdonság miatt az igazoló fél nem kockáztatja titkainak kiszivárgását a bizonyítási eljárás során. Most nekünk is ilyen alkalmazásban lesz szükségünk rájuk. Az alkalmazott nullaismeretű protokollokat az implementációs fejezetben tárgyaljuk.

3. fejezet

A kártyajátékok kriptográfiai modellezése

Feltesszük, hogy a játékosok egymás között egy hiteles üzenetszóró csatornán keresztül kommunikálnak.

3.1. A kártyák reprezentálása

A valós kártyajátékokban egy játékos egy adott szituációban kártyatípusokat, és hátlapokat lát. E két nézetét egy lapnak számértékekkel reprezentáljuk. Míg a valós esetben fizikailag tartozik össze egy kártya típusa és hátoldala, itt az összetartozást függvénykapcsolattal kell megvalósítanunk. Ennek létrehozása során ügyelnünk kell a **Kártyatípusok bizalmas kezelése** célkitűzésünkre. Ezt úgy garantáljuk, hogy szemantikailag biztonságos nyilvános kulcsú rejtjelezőt alkalmazunk. Szükséges továbbá, hogy a hátoldal értékéből a típusérték pontosan akkor legyen kiszámítható, amikor ebbe minden játékos beleegyezik. Ezen követelmények teljesülnek, ha az előző fejezetben bemutatott ElGamal n-ből n küszöb rejtjelezőt (a továbbiakban ElGamal) használjuk a típusérték és a hátoldal közötti függvénykapcsolat létesítésére.
Megjegyezzük, hogy van más rejtjelező is, amely céljainknak megfelelne. Az ElGamal kiválasztásában annak hatékonysága is szerepet játszott, erre még a 6. fejezetben visszatérünk.
A játékosok által az üzenettérből előzetesen kiválasztott típusértékek rejtjelezettjeit kártyakódoknak fogjuk hívni. Mivel a rejtjelező használata során egy-egy típus-

értéket egyedi véletlen elemekkel kódolunk, melyeket szükséges lehet megőrizni a kártyákkal végzett műveletek során, egy kártyát az alábbi három értékkel reprezentálunk:

- típusérték: $d \in G$
- kártyakód: $c = (c_1, c_2) \in G \times G$
- véletlen elem: $r \in \mathbb{R}_q$

Jelölje E az ElGamal rejtést, D a fejtést, E' az újrarejtést. Ekkor a fentiek szellemében $c = E(d, r)$, $d = D(c)$, $c' = E'(c, r)$.
Ha egy játékos kézben tart egy kártyát, akkor szükséges lesz, hogy lapjának mindhárom paraméterét ismerje, míg a többi játékos számára - a nem számítógépes környezetben is lehetséges következtetési lehetőségektől most eltekintve - csak a kártyakód lesz látható. A típusérték mellett a véletlen elem ismerete a fejtéshez ugyan nem feltétel, de bizonyos kártyaműveletekhez szükséges lesz.
Az alábbiakban áttekintjük a következő, implementációs fejezet protokolljainak legfontosabb építőelemeit.

3.2. Műveletek egy kártyával

3.2.1. Típusérték felfedése

Adott egy c kártyakód, keressük a hozzá tartozó típusértéket. Ez az ElGamal fejtés segítségével történik, melyhez az összes játékos közreműködése szükséges. Emiatt teljesül a **Titkos szövetségek minimális hatása** célkitűzésünk.
Ha a típusérték felfedésének célja egy kártya húzása, akkor egy játékos a saját fejtési információját titokban tartja, így a $d = D(c)$ típusértéket egyedüliként tudja meg. Ha a cél egy kézben lévő kártya kijátszása, akkor a fejtési információt ő is nyilvánosságra hozza, így a típusértéket a többi játékos is megtudja.
A játékosok nullaismeretű bizonyításokkal igazolják az elküldött fejtési információk konzisztenciáját a titkos kulcs szétosztott elemeivel.

3.2.2. Kártya létrehozása típusértékből

Egy játékos birtokában van egy d típusérték. Ebből a játékos saját lapot csinál a kártyakód és a véletlen elem létrehozásával. Azaz végrehajtja d-n az ElGamal rejtést, melynek során keletkező r lesz a véletlen elem, amit titokban tart, és $c = E(d, r)$ lesz a kártyakód, amit nyilvánosságra hoz.

3.2.3. Kártyakód cseréje

Egy játékos kicseréli egy nem feltétlenül saját lapjának a kártyakódját egy másikra. Ezt az ElGamal újrarejtés segítségével valósítja meg, melynek eredménye $c' = E'(c, r)$. Az ElGamal rejtjelező leírásánál megmutattuk, hogy ehhez a művelethez nincs szükség az eredeti típusérték, illetve véletlen elem ismeretére. A művelet helyes végrehajtását lehetne nullaismeretű bizonyítással igazolni, de erre nem lesz szükségünk. Ennek az az oka, hogy ezt a műveletet kizárólag egy kártyák csoportjával végzett, következő szakaszban tárgyalásra kerülő művelet részlépéseként alkalmazzuk majd, és e kártyacsoportra vonatkozó művelet helyes végrehajtásának igazolására majd adunk nullaismeretű bizonyítást.

3.3. Műveletek több kártyával

A protokollok tárgyalásakor típusértékek, kártyakódok vagy véletlen elemek rendezett elemtöbbeseivel fogunk dolgozni.
Vezessük be az alábbi jelöléseket:

- típusértékek elemtöbbese: $C = \{c_1, ..., c_n\}$
- kártyakódok elemtöbbese: $D = \{d_1, ..., d_n\}$
- véletlen elemek elemtöbbese: $R = \{r_1, ..., r_n\}$

Értelmezzük az ElGamal műveleteket a fenti elemtöbbeseken az elemenkénti ElGamal műveletek elvégzésével. Pl.: $E(D, R) = C$ jelentse azt, hogy $E(d_1, r_1) = c_1$,..., $E(d_n, r_n) = c_n$.

3.3.1. Keverés

Ez egy összetett eljárás kártyakódok egy C elemtöbbesén. Egy játékos előbb minden egyes elemen elvégzi a **Kártyakód cseréje** műveletet, majd a lecserélt kártyakódok elemtöbbesén végrehajt egy általa választott véletlen π permutációt. A cseréhez használt véletlen értékeket és a permutációt titokban tartja, csak az új kártyakódok $C' = \pi(E'(C, R))$ elemtöbbesét hozza nyilvánosságra. A keverő játékos a régi és az új kártyakódok konzisztenciáját nullaismeretű bizonyítással igazolja.

3.3.2. Szabály ellenőrzés

Nagyon sok szabály követelménye tulajdonképpen meghatározott típusértékek elemtöbbesei közötti tartalmazás reláció fennállása. Ennek igazolását egy ügyes trükkel vissza lehet vezetni a Keverésnél használt nullaismeretű bizonyítás alkalmazására. Ez a művelet fogja teljesíteni a **Csalás észrevétele nagy valószínűséggel** célkitűzésünket.

Mivel e szakaszban csak a legfontosabb építőelemekre kívánunk szorítkozni, és beérjük az előző szakaszban felvázolt kriptográfiai apparátus beépítésének illusztrálásával, ezt a műveletet részletesebben a következő, implementációról szóló fejezetben tárgyaljuk.

4. fejezet

A tarokk implementációja

Ebben a szakaszban megadjuk az implementáció kriptográfiával kapcsolatos protokolljait. Nem térünk itt ki egy gyakorlati implementáció azon részeire, melyek nem hozhatók közvetlenül kapcsolatba a célkitűzéseknél felsorolt biztonsági követelményeinkkel. Ilyen például annak eldöntése, hogy egy adott ütést ki visz el, vagy ilyen az ütésértékpontok számolása, amely a játéknak szintén fontos eleme, hiszen a játék nyerteseinek kiléte is gyakran ennek függvénye. Azonban ezen feladatok megoldása és illesztése az alábbi implementációhoz nem igényel kriptográfiával kapcsolatos megfontolásokat.

Az alábbi protokollok és eljárások fejlécénél a

Protokoll neve (input paraméterek) illetve a

Protokoll neve (input paraméterek; output paraméterek)

jelölést alkalmazzuk, ez alól az **Inicializálás** protokoll kivételt fog képezni: az általa létrehozott paramétereket globális értékekként kezeljük, melyek a további protokolloknak és eljárásoknak mindig rendelkezésre állnak. Az i. játékost $\mathcal{P}_i$-vel jelöljük. A jobb áttekinthetőség érdekében az olyan lépések sorozatát, amelyeket egymás után, azonos módon hajtanak végre az egyes játékosok, ciklusokká szervezzük. Ez természetesen implementációs szempontból nem helyes, hiszen ilyenkor a ciklusmag rendre különböző gépeken fut le.

4.1. Inicializálás

Ebben a protokollban kap helyet az ElGamal kulcslétrehozó algoritmusa, a nullaismeretű protokollok végrehajtásában szerepet játszó s biztonsági paraméter értékének definiálása, a típusértékek definiálása, és nyílt rejtjelezésük létrehozása a $C_0 = E(D, 1)$ művelettel, ahol most 1 a megfelelő méretű csupa 1 elemtöbbest jelenti. A nyílt rejtjelezésnek termeszétesen nincs valódi elrejtő szerepe, de a továbbiakban szükség lesz rá, és itt teljesül **Kártyák egyedisége** célkitűzésünk.

1. A játékosok megállapodnak a p és q prímekben, melyekre $p = 2q + 1$ teljesül. Legyen G a mod p kvadratikus maradékok csoportja. (Ekkor G rendje q.)

2. A játékosok választanak egy $g \in G$ generátorelemet.

3. Ciklus: i = 1-től 4-ig:
   $\mathcal{P}_i$ létrehoz magának egy véletlen $x_i \in \mathbb{Z}_q$ titkos kulcsot.
   $\mathcal{P}_i$ közzé teszi a saját $h_i = g^{x_i}$ nyilvános kulcsát.
   Ciklus (i) vége

4. A játékosok kiszámolják a közös nyilvános kulcsot: $h = \prod_{i=1}^{4} h_i$

5. A játékosok megállapodnak egy s biztonsági paraméterben.

6. A játékosok megállapodnak 42 értékben, melyek a típusértékeket reprezentálják: $D_0 = \{d_1, ..., d_{42}\}$

7. A játékosok létrehozzák a típusértékek nyílt rejtjelezését:
   Ciklus: i = 1-től 42-ig:
   $c_{i,1} = g$
   $c_{i,2} = d_i h$
   $c_i = (c_{i,1}, c_{i,2})$
   Ciklus (i) vége

8. $C_0 = \{c_1, ..., c_{42}\}$

Az alábbi protokollok egy része pontosan az előző fejezetben megadott kártyaműveleteket valósítja meg, amit az elnevezések egyeztetésével teszünk egyértelművé. A protokollok nagyobb része lazább kapcsolatban van a kártyaműveletekkel, ebben az esetben a protokoll leírását is megadjuk.

4.2. Protokollok egy kártyával

4.2.1. Kártya létrehozása típusértékből (d; $c = (c_1, c_2)$, r)

1. $\mathcal{P}_i$ választ egy véletlen $1 < r < q$ értéket
2. $\mathcal{P}_i$ kiszámolja $c_1 = g^r$-et, és $c_2 = dh^r$-et
3. $\mathcal{P}_i$ közzéteszi $c = (c_1, c_2)$-t, titokban tartja r-et.

4.2.2. Diszkrét logaritmusok egyenlőségének igazolása (x, y, g, h, α)

Ez a két **Típusérték felfedése** jellegű, a következőkben tárgyalásra kerülő protokoll által használt nullaismeretű bizonyítás. Igazolja két G-beli elem g alapú diszkrét logaritmusának egyenlőségét, és a diszkrét logaritmus értékének ismeretét. Azaz, ha $x = g^\alpha$ és $y = h^\beta$, akkor az igazoló ismeri α-t, és $\alpha = \beta$.

1. $\mathcal{P}_j$ választ egy véletlen $\omega \in \mathbb{Z}_q$ elemet, és titokban tartja
2. $\mathcal{P}_j$ kiszámolja és közzéteszi $(a, b) = (g^\omega, h^\omega)$-t
3. Az ellenőrző játékosok közösen választanak egy $c \in \mathbb{Z}_q$ elemet, és elküldik c-t $\mathcal{P}_j$-nek
4. $\mathcal{P}_j$ kiszámolja és közzéteszi $r = \omega + \alpha c \pmod q$-t

Az ellenőrző játékosok pontosan akkor fogadják el az igazolást, ha $g^r = ax^c$ és $h^r = by^c$ teljesül.

4.2.3. Kártya húzása ($c = (c_1, c_2)$; d)

Ez az egyik **Típusérték felfedése** jellegű protokoll, itt a kártyát húzó játékos a laphoz tartozó fejtési információját titokban tartja. A paraméterek átadásának helyességének igazolása az előbb tárgyalt nullaismeretű protokoll meghívásával történik.

1. Ciklus: $j = 1$-től 4-ig, $j \neq i$:
   $\mathcal{P}_j$ kiszámolja és közzéteszi $e_j = c_1^{x_j}$-t
   $\mathcal{P}_j$ elvégzi a **Diszkrét logaritmusok egyenlőségének igazolása** (e_j, h_j, c_1,

g, x_j) protokollt

Ciklus (j) vége

2. $\mathcal{P}_i$ kiszámolja e_i=$c_{t,1}^{x_i}$-t

3. $\mathcal{P}_i$ kiszámolja $d = c_2 / \prod_{k=1}^{n} e_k$-t, így megtudja a lapjának értékét.

4.2.4. Kártya kijátszása ($c = (c_1, c_2)$)

Ez a másik **Típusérték felfedése** jellegű protokoll, ahol minden játékos közzéteszi a laphoz tartozó fejtési információját. A paraméterek átadásának helyességének igazolása itt is az előbb említett nullaismeretű protokoll meghívásával történik.

1. Ciklus: j = 1-től 4-ig:

   $\mathcal{P}_j$ kiszámolja és közzéteszi $e_j = c_1^{x_j}$-t

   $\mathcal{P}_j$ végrehajtja a **Diszkrét logaritmusok egyenlőségének igazolása** (e_j, h_j, c_1, g, x_j) protokollt

   Ciklus (j) vége

2. Ciklus: j = 1-től 4-ig:

   $\mathcal{P}_j$ kiszámolja $d = c_2 / \prod_{k=1}^{n} e_k$-t, így megtudja a lap értékét.

   Ciklus (j) vége

4.3. Protokollok kártyák csoportjaival

4.3.1. Keverés ($C = \{c_1, ..., c_{42}\}$; C', π, R)

1. $\mathcal{P}_i$ választ egy véletlen π permutációt

2. Ciklus: j = 1-től 42-ig:

   $\mathcal{P}_i$ választ egy véletlen $1 < r_j < q$ értéket

   $c'_{j,1} = c_{j,1} g^{r_j}$

   $c'_{j,2} = c_{j,2} h^{r_j}$

   $c'_j = (c'_{j,1}, c'_{j,2})$

   Ciklus (j) vége

3. $C' = \{c'_{\pi(1)}, ..., c'_{\pi(42)}\}$

4. $R = \{r_1, ..., r_{42}\}$

4.3.2. Keverés ellenőrzése (C, C', π, R)

Ez az eljárás a következő, **Keverés igazolása** nullaismeretű protokoll ellenőrzésre vonatkozó része.

1. Ciklus: j = 1-től 42-ig:
   $c''_{i,1} = c_{i,1} g^{r_i}$
   $c''_{i,2} = c_{i,2} h^{r_i}$
   $c''_i = (c''_{i,1}, c''_{i,2})$
   Ciklus (j) vége

2. $C'' = \{c''_{\pi(1)}, ..., c''_{\pi(42)}\}$

Az ellenőrző játékosok pontosan akkor fogadják el a keverést, ha $i = 1, ..., 42$ esetén $c'_{i,1} = c''_{i,1}$ és $c'_{i,2} = c''_{i,2}$ teljesül.

4.3.3. Keverés igazolása (C, C', π, R)

Ez a protokoll egy nullaismeretű bizonyítás a **Keverés** protokoll helyes elvégzésére. A **Keverés** protokoll után minden esetben azonnal végre kell hajtani. Egy csaló igazoló fél $1/2^s$ valószínűséggel nem bukik le.

1. Ciklus: j = 1-től s-ig:
   $\mathcal{P}_i$ elvégzi a **Keverés** (C'; C_j, π'_j, R'_j) protokollt
   $\mathcal{P}_i$ közzéteszi C_j-t
   Ciklus (j) vége

2. Az ellenőrző játékosok közösen választanak egy véletlen $S \subset \{1, ..., s\}$ halmazt, és elküldik S-et $\mathcal{P}_i$-nek

3. Ciklus: j = 1-től s-ig:
   Ha $j \in S$:
   $\mathcal{P}_i$ közzéteszi π'_j-t és R'_j-t.
   Az ellenőrző játékosok végrehajtják a **Keverés ellenőrzése** (C', C_j, π'_j, R'_j) eljárást

Feltétel vége

Ha $j \notin S$:

$\mathcal{P}_i$ kiszámolja $\pi_j = \pi \circ \pi_j^{'}$-t

$\mathcal{P}_i$ kiszámolja $R_j = \{r_{j,1}, ..., r_{j,42}\}$-t, ahol $k = 1, ..., 42$ esetén $r_{j,k} = r_{j,k}^{'} + r_{\pi(j)}$

$\mathcal{P}_i$ közzéteszi π_j-t és R_j-t

Az ellenőrző játékosok végrehajtják a **Keverés ellenőrzése** (C, C_j, π_j, R_j) eljárást

Feltétel vége

Ciklus (j) vége

4.3.4. Osztás (C_0; D^1, C^1, R^1,..., D^4, C^4, R^4)

Ez a művelet úgy megy végbe, hogy a játékosok egymás után végrehajtják a **Keverés** protokollt. Ha egy játékos nem keverné meg a lapokat, azzal kockáztatná, hogy a többiek összefogva ismerjék a lapjait. Ezt követően a megkevert lapokat kiosztjuk a szabályoknak megfelelően. Ennek első lépéseként a **Kártya húzása** protokoll ismételt alkalmazásával minden játékos megismeri lapjainak típusértékét. Mivel a **Keverés** többszöri alkalmazása a véletlen elemeket is elrejtette mindenki elől, a **Kártya létrehozása típusértékből** protokoll segítségével új kártyakódokat kell létrehozni, melynek során létrejönnek az új, privát véletlen elemek is. Ez a protokoll teljesíti **Kártyák véletlenszerűsége, egyenletes eloszlás szerint** célkitűzésünket.

1. Ciklus: i = 1-től 4-ig:

   $\mathcal{P}_i$ elvégzi a **Keverés** (C_{i-1}; C_i, π_i, R_i) protokollt

   $\mathcal{P}_i$ közzéteszi C_i-t, de titokban tartja π_i-t és R_i-t

   $\mathcal{P}_i$ elvégzi a **Keverés igazolása** (C_{i-1}, C_i, π_i, R_i) eljárást

   Ciklus (i) vége

2. A megkevert pakli $C_4 = \{c_{4,1}, ..., c_{4,42}\}$

3. Ciklus: i = 1-től 4-ig:

   Ciklus: j = 1-től 9-ig:

   $\mathcal{P}_i$ végrehajtja a **Kártya húzása** ($c_{4,9(i-1)+j}$; d_j^i) protokollt

   $\mathcal{P}_i$ végrehajtja a **Kártya létrehozása típusértékből** (d_j^i; c_j^i, r_j^i) protokollt

Ciklus (j) vége

Ciklus (i) vége

4.3.5. Szabály ellenőrzés (C, D, R, C_0', D_0')

Az alábbi, a szabályok betartásának játék közbeni ellenőrzéséhez használható protokollban C az aktuális szabálytól függően jelölheti:

- $\mathcal{P}_i$ egyetlen lapjának kódját
- $\mathcal{P}_i$ összes lapjának kódját
- $\mathcal{P}_i$ lapjai kódjainak egy általa kiválasztott és megjelölt részét

A C elemeihez tartozó típusértékek elemtöbbesét jelölje D, véletlen elemek elemtöbbesét jelölje R.
Emlékeztetőül, D_0 az **Inicializálás** során a játékosok közös megegyezésével létrehozott típusértékek elemtöbbese, C_0 pedig ennek nyílt rejtjelezése, melynek elemeihez minden játékos egyértelműen hozzá tudja rendelni annak D_0-beli párját.
A szemléletesség kedvéért jelölje $C_0' \subset C_0$ az aktuális szabály ellenőrzéséhez használt kártyaértékek elemtöbbesének nyílt rejtjelezését, a C_0' elemeihez tartozó kártyaértékek elemtöbbesét jelölje D_0'.
A protokollban tulajdonképpen a $D \subset D_0'$ tartalmazásra adunk nullaismeretű bizonyítást. Ennek első lépéseként C-hez hozzávesszük $D_0' \setminus D$ típusértékeinek egy rejtjelezését, így kapjuk C'-t. A C'-höz tartozó típusértékek elemtöbbesét jelölje D'.
Az igazolni kívánt tartalmazás pontosan akkor áll fenn, ha C_0' és C' a keverés eljárással egymásba vihetők. Vagyis a viszonyuk megegyezik C_0 és a játék elején $\mathcal{P}_1$ által az **Osztás** eljárásban létrehozott C_1 viszonyával. Így nincs más hátra, mint elvégezni a **Keverés igazolása** eljárást.
Tegyük fel, hogy $\mathcal{P}_i$ egy adott pillanatban köteles lenne tarokkot tenni, de nincs nála, és színes lapot tesz. Ekkor igazolnia kell, hogy nincs a kezében tarokk. Ebben az esetben a protokoll paraméterezése:
$C = \mathcal{P}_i$ összes lapjának kódja
$D = \mathcal{P}_i$ összes lapjának típusértékei
$R = \mathcal{P}_i$ összes lapjának véletlen elemei

$C_0^{'}$ = színes lapok kódjai a nyílt rejtjelezésében

$D_0^{'}$ = színes lapok típusértékei a nyílt rejtjelezésében

1. $D_0^{'} \setminus D = D^{-}$
2. $k = |D| \qquad k^{-} = |D^{-}|$
3. Ciklus: $j = 1$-től k-ig:

   $d_j^{'} = d_j$

   $c_j^{'} = c_j$

   $r_j^{'} = r_j - 1$

   Ciklus (j) vége
4. Ciklus: $j = 1$-től k^{-}-ig:

   $\mathcal{P}_i$ választ egy véletlen $1 < r_j^{-} < q$ értéket

   $d_{k+j}^{'} = d_j^{-}$

   $c_{k+j,1}^{'} = g^{r_{k+j}^{-}}$

   $c_{k+j,2}^{'} = d_{k+j}^{'} h^{r_j^{-}}$

   $c_{k+j}^{'} = (c_{k+j,1}^{'}, c_{k+j,2}^{'})$

   $r_{k+j}^{'} = r_j^{-} - 1$

   Ciklus (j) vége
5. $D^{'} = \{d_1^{'}, ..., d_{k+k^{-}}^{'}\}$
6. π legyen az a permutáció, melyre $\pi(D_0^{'}) = D^{'}$
7. $C^{'} = \{c_1^{'}, ..., c_{k+k^{-}}^{'}\}$
8. $R^{'} = \{r_1^{'}, ..., r_{k+k^{-}}^{'}\}$
9. $\mathcal{P}_i$ elvégzi a **Keverés igazolása** ($C_0^{'}$, $C^{'}$, π, $R^{'}$) eljárást.

5. fejezet

Igazolás

Ebben a szakaszban végig követjük a játék menetét, és a sorra kerülő, kriptográfiai szempontból feladatot jelentő elemeket rendre ellátjuk a fenti implementációban a feladatot megoldó protokollokra való hivatkozásokkal. Ezúton igazoljuk, hogy a tárgyalt, célkitűzéseinkkel összhangban lévő implementáció illeszkedik a tarokk játék menetéhez és szabályaihoz.
A most következő részben gyakran utalunk a függelékben található szabályismertető számos pontjára. A játék öt részre tagolható, úgy mint: előkészítő fázis, licitálás, talon csere, figurák bemondása illletve lejátszás, ahogyan ez további alfejezeteinkben is megjelenik.

5.1. Előkészítő fázis

A játék az **Inicializálás** protokoll lefutásával veszi kezdetét.
A játék első fontos eleme a helyválasztás. Ezt a szabályismertetőben leírtaktól eltérően valósíthatjuk meg a játékosok egy véletlen permutációjának kiválasztásával. A lapok szétosztása az **Osztás** protokoll segítségével történik. Itt lesz először szükségünk a **Keverés** protokollra, melyet minden esetben azonnal a **Keverés igazolása** nullaismeretű protokoll követ, ezt a továbbiakban nem említjük. A lapok szétosztása a **Kártya húzása** és a **Kártya létrehozása típusértékből** protokollok segítségével valósul meg.

5.2. Licitálás

A licitálás során kerül először a **Szabály ellenőrzés** protokoll használatára, hiszen aki licitál, annál - egy kivételes esettől eltekintve - kell, hogy legyen honőr.
A konvencionális licitmenetek (invit illetve engedett játék) elhangzásukkor kötelező jelleggel szintén lapot jeleznek. Ezek jelentésének betartása szabály, mely újra az előző protokollal ellenőrizhető.
A szabályellenőrzések miatt a talon csere előtt a licitáló játékosoknak el kell végezniük a **Keverés** protokollt saját lapjaikon, hogy más játékos ne tudja, hogy melyik lapjuk a jelzett honőr. A végrehajtás során a kártyakódokhoz tartozó véletlen elemek változását követni kell.

5.3. Talon csere

A talon lapjainak felhúzására a **Kártya húzása** szolgál, melyben a fejtési paraméterek helyességére a **Diszkrét logaritmusok egyenlőségének igazolása** protokoll ad nullaismeretű bizonyítást.
A lapok letételéhez nincs szükség kriptográfiai protokollra, ez a megfelelő kártyakódok megjelölésével, és a kártyakód talonhoz csatolásával történik. A talon letételét minden esetben a **Szabály ellenőrzés** protokoll követi. Tarokk fektetése esetén igazolni kell, hogy a fektetett lap tarokk, de nem honőr. Ha a felvevő fektetett tarokkot, akkor miután mindenki letett, a **Kártya kijátszása** protokollal fedi fel a tarokk értékét. Ha nem történik tarokk fektetés, akkor azt kell igazolni, hogy a fektetetett lapok színesek, de nem királyok. Meg kell említenünk még a játék eldobásának lehetőségét, melyre feljogosító lapösszeállítást szintén a **Szabály ellenőrzés** protokollal ellenőrzünk.

5.4. Figurák bemondása

A "8 tarokk" és "9 tarokk" bemondásokat a **Szabály ellenőrzés** protokollal ellenőrizzük. Mivel 9 tarokkal nem lehet 8 tarokkot mondani, az előbbi esetben kétszer kell alkalmazni a protokollt: azt is igazolni kell, hogy a 9. lap színes. Mivel pagátulti bemondása és kontrázása esetén kötelező a magas tarokkszám jelzése, ezért abban

az esetben, ha ezen bemondásokat megelőzően nem hangzott el "8 tarokk" vagy "9 tarokk" jelzés, igazolni kell 2 színes lap birtoklását. Aki ilyen igazolást végez, annak utána saját lapjai el kell végeznie **Keverés** protokollt a véletlen elemek követésével, hogy a többi játékos ne tudja, hogy hol vannak a jelzett színes lapjai. A felvevő partnerének igazolnia kell, hogy valóban övé a meghívott a tarokk. Ha a felvevő megszólalása után "kontra" hangzik el, akkor a bemondó ugyanígy igazolja, hogy nem övé a meghívott tarokk.

5.5. Lejátszás

Az eddig csak kivételes esetben használt **Kártya kijátszása** protokoll itt központi szerepű. Az egyes körökben az elsőnek asztalra kerülő lap kijátszása előtt nem, de az utána kijátszott lapok letétele előtt a szín- és adukényszer szabályok miatt gyakran szükség van a **Szabály ellenőrzés** protokollra is. Itt ez a protokoll a paraméterként kezelt kártyahalmazok szempontjából három féle alakot ölthet:

- "Színt teszek."
- "Nincs színem, tarokkot teszek." Itt a protokollra egymás után kétszer is szükség van.
- "Nincs színem, és tarokkom se."

Ezekhez társulhat még egy negyedik eset: ha be lett mondva pagátulti, és a bemondóknál van a pagát, akkor a birtokosa köteles meghagyni azt utolsó tarokkjának. Vagyis ilyenkor a fentiek mellé beékelődik még ez a lehetőség:

- "Pagátot teszek, és nincs több tarokkom." Itt is kétszer van szükség a protokollra.

Nincs szükség szabály ellenőrzésre az utolsó körben, illetve akkor, ha a lejátszás menete más okból egy ponton ezt fölöslegessé teszi. Ilyen eset például, ha egy színre valaki egyszer már tarokkot tett, és újra hívja valaki azt a színt, akkor a fenti második esetből a "Nincs színem" kitétel elhagyható. Vagy ha se szín, se tarokk nem volt már az előző körök valamelyikében sem, akkor nincs mit igazolni.
Miután a játékosok lapjai elfogytak, következik az ütésértékpontok összeszámolása.

Ehhez szükség van a talonban lévő lapok típusértékeinek felfedésére. Ezt ugyancsak a **Kártya kijátszása** protokoll segítségével végezzük el, annak ismételt alkalmazásával.

Ezután már csak a játék nyerteseinek és díjazásának megállapítása van hátra. Ezt a részt feleslegesnek éreztük protokollokkal fedni, ahogyan azt az implementációs rész elején már megjegyeztük.

6. fejezet

A szakirodalom áttekintése

6.1. A kártyajátékok és a nyilvános kulcsú kriptográfia

A "Mental Poker" probléma nagyjából egyidős a nyilvános kulcsú kriptográfiával. Eleinte a póker megbízható fél nélküli implementálását tűzték ki célul. Már Rivest, Shamir és Adleman foglalkozott a problémával 1979-ben, nem sokkal a híres RSA algoritmus publikálása után. De az ő RSA függvényre épülő megoldásuk nem volt biztonságos, mert az egyszerű RSA függvény információt fed fel egyes bitekről. Ez a megfigyelés vezette el Goldwassert és Micalit a szemantikai biztonság fogalmának megalkotásához, és a nyilvános kulcsú kriptográfiában a véletlen használatának bevezetéséhez. Így vezetett el a "Mental Poker" a bizonyítható biztonság témaköréhez.

6.2. Implementációk a protokollok leírásával

Crepeau póker protokolljainak sikerült először 1987-ben elérnie azt, hogy a játék végén ne kelljen nyilvánosságra hozni a lapokat. Ez alapvető követelmény, hogy a játékosok stratégiája titokban maradhasson.
Először Schindelhauer foglalkozott más kártyajátékok implementálásának a gondolatával 1998-as cikkében. Crepeau ötletét kiterjesztve kidolgozta a legtöbb kártyajáték által igényelt protokollok rendszerét. Figyelmét nem kerülte el a szabály ellenőrzés gondolata sem, és részletesen kidolgozta a kártyák csoportjai közötti tartalmazásra való visszavezetés általunk is használt ötletét.

Schindelhauer megvalósításának hátránya, hogy akárcsak Crepeau, ő is a Goldwasser-Micali rejtjelezőt használja. Ez a rejtjelező ugyan szintén szemantikailag biztonságos, de nagy tárigénye miatt a gyakorlatban nemigen alkalmazható. Bitenkénti rejtjelezést használ, és ezáltal egy kártya rejtjelezéséhez felhasznált bitek száma lineárisan függ a játékosok számától és logaritmikusan a kártyapakli méretétől. Az általunk ismertetett, ElGamalra épülő módszerrel ezek a függések eltűnnek, ahogyan arra Barnett és Smart később, egy 2003-as cikkben rámutatnak. Ez utóbbi cikk alternatívaként kínálja még a hasonló hatékonyságú Paillier rejtjelezőt is. Barnett és Smart cikke absztrakt megközelítéssel, hatékony kriptográfiai eszközöket mutat be az implementációhoz. Hátránya, hogy nem adja meg a felvázolt protokollok implementációhoz közeli leírását, ahogyan ezt Castella-Roca később megjegyzi, bár hivatkozásokat közöl. A szabály ellenőrzés lehetőségét felveti, de ezen a ponton különösen szűkszavú a tárgyalásmód, és a hivatkozások áttekintésével sem tűnik rekonstruálhatónak a probléma megoldásával kapcsolatos elképzelésük.

Castella-Roca póker implementálásának szentelt 2005-ös doktori dolgozata saját eredményeinek tárgyalása mellett széleskörű betekintést nyújt a terület szakirodalmába. Az eredményeket biztonsági követelményeiknek való megfelelésük szerint csoportosítja, és elvégzi az egyes csoportok összehasonlító kommunikációs tár és számítási idő szerinti költségelemzését. Ennek keretei között foglalkozik Barnett és Smart munkájával is, és megadja a pókerrel kapcsolatos protokollok implementációját. Mi is ezt a megközelítését alkalmaztuk, és a protokollok algoritmikus leírását kiterjesztettük a tarokk szabályai által megszabott feladatok implementálására.

6.3. Hatékonyság és biztonság

Barnett és Smart a gyorsítás érdekében használja az interaktív nullaismeretű bizonyítások nem interaktívvá tételét egy hash-függvény segítségével. Ez a más célból is gyakran alkalmazott Fiat-Shamir transzformáció segítségével történik, melynek biztonságtartó tulajdonságát az utóbbi időben megkérdőjelezték. Pointcheval és Stern korábban még azt bizonyították, hogy a Fiat-Shamir transzformáció megőrzi a biztonságot a véletlen orákulum modellben. Ez azt jelenti, hogy a hash függvény szerepét egy véletlen orákulum játssza. De Goldwasser és Kalai konstruált olyan interak-

tív protokollt, amelyre a Fiat-Shamir transzformációt tetszőleges hash-függvénnyel alkalmazva a kapott nem interaktív protokoll a standard modellben már nem biztonságos. Persze ez nem jelenti azt, hogy esetleg a mi protokolljainkra alkalmazva sem őrizné meg a biztonságot, csupán annyit, hogy az eddigi eredmények értelmében bizonyított biztonságról a nem interaktív protokoll esetén már nem beszélhetünk. Ezzel együtt a gyakorlatban megfontolandó lehet engedni a bizonyítható biztonság kritériumából a hatékonyság növelése érdekében, természetesen fenntartva azért egy véletlen orákulum modellbeli, a standard modell szemszögéből intuitív biztonságot.

6.4. Számítógépes megvalósítás

Az első számítógépes megvalósítás Stamer nevéhez fűződik. 2005-ben Schindelhauer protokolljait, valamint Barnett és Smart ElGamal alapú kártyakódjait ültette át a gyakorlatba, a futási időket a Fiat-Shamir transzformáció alkalmazásával és néhány gyorsítási eljárással javítva. Szabad szoftverként létrehozott absztrakt C++ osztálykönyvtárának működését a 32 lapos kártyával játszható német Skat kártyajáték implementálásával illusztrálta. Bebizonyította, hogy téves az a hit, mely szerint a megbízható féltől való megszabadulás a számítási idők elviselhetetlen növekedésével járna. A legköltségigényesebb eljárást, az osztást a helyesség ellenőrzésével együtt sikerült megfelelő biztonsági szinten 20 másodperc alá szorítania. Ennek ellenére, ahogy összefoglalójában megjegyzi, nem valószínű, hogy a működő internet kaszinók áttérnének a játék tisztaságát erős kriptográfiai eszközökkel garantáló, nyilvánosan ellenőrizhető, szabad szoftverek használatára. Mégis, ez az irány a jövőben az internetkapcsolatok sebességének további növekedésével érdeklődésre tarthat számot, nem beszélve olyan egyéb alkalmazásokról, ahol nem is állhat rendelkezésre megbízható fél.

7. fejezet

FÜGGELÉK - A magyar tarokk szabályai

Jelen szabályismertető teljes változata a
http://www.pagat.com/tarot/xx-hi_hu.html
internetcímen érhető el. A kivonatolás során elsősorben arra törekedtünk, hogy semmiképpen ne maradjon ki lényeges részlet a szabályok leírásából. Bár az eredeti terjedelmet jelentősen csökkentettük, e fejezet jóval bővebb, mint amennyit kriptográfiával kapcsolatos implementációnk megkívánna.

7.1. Játékosok és a kártya

7.1.1. A játékosok

A tarokk tulajdonképpen négyszemélyes játék, hiszen egyidőben négyen vesznek részt ténylegesen a játékban. Ugyanakkor szokásos ötösben játszani, amikor is az osztó kimarad a játékból. (Ilyenkor alkalma nyílik italt kínálni, tölteni stb.) Az összes többi tarokkjátékhoz hasonlóan a magyar tarokk is ütéseken alapuló játék. Az együtt játszó párok összeállítása partiról-partira változik, aszerint hogy a licitet megnyerő játékos által meghívott lap kinek a kezében van.

7.1.2. A kártya

A játékhoz 42 lapos kártyacsomag szükséges. Négyféle színes lap van (kőr, káró, treff és pikk), továbbá 22 tarokk, amelyek aduként szolgálnak. A tarokk-kártya rendesen 54 lapos

csomagban kapható, amelyben az egyes színekből 8-8 található - ezekből kell eltávolítani 3-3-at úgy, hogy a fekete színekből a 7-est, a 8-ast és a 9-est, míg a pirosakból a 2-est, a 3-ast és a 4-est vesszük ki. Így jutunk a játékhoz szükséges 42 laphoz.

Az egyes lapok pontértékekkel rendelkeznek: a játék elsődleges célja a pontok többségének ütésekben történő hazavitele, ezáltal a parti megnyerése. A legnagyobb tarokkot skíznek nevezzük; kinézetre leginkább Jokerre hasonlít. A többi tarokk római számmal van jelölve: kezdve a XXI-esen, amely a második legmagasabb tarokk, egészen le az I-esig, amelynek külön neve is van: pagát. A skíz, a XXI-es és a pagát kitüntetett lapok, honőröknek nevezzük őket. Pontértékük egyenként 5. A skízt és a XXI-est nagyhonőrként szokás emlegetni. A többi tizenkilenc tarokk, a XX-astól a II-esig 1-1 pontot ér.

A színek fajtánként 5-5 lapból állnak. A fekete színekben a lapok rangsorban föntről lefelé a következők: király, dáma, lovas, bubi vagy botos, tízes. A piros színek lapjai rangsorban föntről lefelé: király, dáma, lovas, bubi vagy botos, ász. Jóllehet a lapok sarkában nincs jelölés, elég könnyen megkülönböztethetők: a király koronát visel, a dáma női alak, a lovas lovon ül, a bubi lándzsát ill. buzogányt tart. A színes lapok pontértéke a következő:

- király: 5 pont
- dáma: 4 pont
- lovas: 3 pont
- bubi: 2 pont
- tízes ill. ász: 1 pont

A kártyacsomag lapjainak összértéke 94 pont: ebből négyszer 15 az egyes színekben található, 15-öt érnek összesen a honőrök, a többi 19-et pedig a maradék tarokkok adják.

7.2. A játék nagy vonalakban

A játék teljes egészében az óramutató járásával ellentétes irányban zajlik. Az osztáskor a négy tényleges játékos elé 9-9 lap kerül, míg a maradék 6 képpel lefelé fordított lap alkotja a talont. Ekkor licitálás következik, ahol a lehetséges licitek a következők (növekvő értéksorrendben): "három", "kettő", "egy" és "szóló". A licit nyertese (a "felvevő") bizonyos számú lapot vesz föl a talonból, majd azonos számú lapot tesz le. A nyerő licit egyben meghatározza a felvevő által a talonból vett lapok számát - a "szóló" nulla lapot jelent. A talon további lapjaiból a többi három játékos a lehető legarányosabban részesül, majd ők

is annyi lapot tesznek le, hogy végül ismét kilenc lap legyen a kezükben.

Az együtt játszó párok összetétele partiról-partira változik. A felvevő meghív egy tarokkot - rendes körülmények között a XX-ast -, minekutána a meghívott tarokkot tartó személy a partnerévé válik, anélkül hogy ezt a tényt bejelentené. A másik két játékos alkotja az ellenpártot. Gyakorta megesik, hogy csak a lejátszás során derül ki, ki kivel van - például ha a meghívott kártyát kijátsszák. Máskor a partnerek kiléte kikövetkeztethető a licitálásból vagy az azt követő bemondásokból.

Miután a felvevő partnert hívott, a bemondások következnek. A felvevő után a többi játékos következik, minek során: bemondhatják nyolc vagy kilenc tarokkjukat; bemondhatnak egy vagy több figurát; megkontrázhatják a játékot, illetve bármely korábban az ellenfél részéről bemondott figurát, amelyről úgy gondolják, hogy el fog bukni. Ezt követően az első lapot az osztótól jobbra ülő játékos hívja ki. Színre ugyanolyan színt kell tenni, ha pedig a hívott színből nincsen, tarokkot. Ha mind a kilenc ütés megvolt, megszámolják a hazavitt ütésekben lévő pontokat. Ha a felvevő és partnere ütötte a pontok többségét (azaz legalább 48-at), akkor ők nyertek. A parti befejeztével azonnal fizetni kell, általában pénzben, néha papíron vezetett elszámolásban. A játékon kívül egyéb figurák is díjazásban részesülnek: így ha valamelyik fél ütéseiben az összes honőrt vagy mind a négy királyt hazaviszi, ha a pontok háromnegyed részét eléri, ha az utolsó ütést a pagáttal viszi haza, vagy ha az ellenfél XXI-esét skízével elfogja. A figurák jutalma gyakran magasabb magának a játék megnyerésének díjazásánál. Ha az illető figurát előzetesen bemondták, a díjazás kétszeres; hasonlóképpen kétszeresen kell fizetni azt a bemondást, amelyet megkontráztak.

7.3. Helyválasztás, osztás, a játék befejezése

A játékosok egymáshoz viszonyított pozíciója fontos szerepet kap a játék során, ezért az ülésrendet sorsolás útján szokták kialakítani, a következő eljárással. Kivesznek a pakliból egy tarokkot, továbbá minden színből egy lapot (öt játékos esetén), illetve egy tarokkot és három különböző színt (ha négyen játszanak). A lapokat megkeverik, és képpel fölfele az asztalra osztják. Ezután egy ezzel azonos módon összeállított lapsort - egy tarokkot és három vagy négy különböző színt - osztanak ki a játékosoknak, képpel lefelé. A játékosok megnézik lapjukat, és arra a helyre ülnek, ahol az ő színüknek (tarokkjuknak) megfelelő lap fekszik. Az a játékos kezdi a licitálást ill. lesz az induló az első partiban, akinek a tarokk jutott. A tőle balra ülő játékos az első osztó ("tarokknak osztanak").

A játék teljes egészében az óra mutatójának járásával ellentétesen zajlik. Ha négyen játsza-

nak, mindenki részt vesz minden játszmában. Ha a játékosok száma öt, az osztó kimarad - az ő szerepe az osztásra korlátozódik. Az osztó először megkeveri a kártyát, a tőle balra ülő játékos pedig emel. Az osztás során az osztó először hat lapot helyez az asztal közepére képpel lefele: ez a talon. Ezt követően mind a négy tényleges játékos 5-5 lapot kap az osztó jobbján ülőn kezdve az óramutató járásával ellentétes irányban, majd ugyanígy továbbhaladva a játékosok további 4-4 lapot kapnak.

A parti lejátszását és a fizetést követően az osztás az osztótól jobbra ülő játékosra száll.

A tarokkozást a "skíz oszt, nem oszt" hagyományos eljárás keretében szokták befejezni. A módszer a következő: Miután valamelyik játékos bemondta a "skíz oszt, nem oszt"-ot, a következő partiban megfigyelik, kihez került a skíz. Ezután a játék folytatódik, míg az illető sorra kerül az osztásban (a skíz oszt), majd ezt követően még egy kört, de ezt már úgy, hogy a szóbanforgó játékostól balra ülő játékos lesz az utolsó osztó (a skíz nem oszt). A játék ezen a ponton ér véget. A "skíz oszt, nem oszt" bemondása után ezek szerint öt játékos esetén 5-9 játszma következhet - ha négyen játszanak, ez a szám 4-7, aszerint hogy hová kerül a skíz.

Noha bármelyik játékos bemondhatja a "skíz oszt, nem oszt"-ot, szokás szerint a játék befejezésére olyan játékos tesz javaslatot, aki vesztésben van. Persze külön eljárás nélkül is be lehet fejezni a tarokkozást, ha a játékosok ebben egyetértenek.

7.4. A licitálás

Hogy ki lesz a felvevő, árverés útján dől el. A licitálást az osztótól jobbra ülő játékos kezdi, majd a többiek következnek az óramutató járásával ellentétesen. A négy lehetséges licit egyben mutatja azon lapok számát (nullától háromig), amelyet a licitálás győztese a talonból cserélhet majd. Minél kevesebb lapot cserél a győztes, annál magasabb a licit, és a játék díjazása is annál nagyobb. A licitek növekvő sorrendben:

- három (a játék díjazása 1 pont);
- kettő (a játék díjazása 2 pont);
- egy (a játék díjazása 3 pont);
- szóló (a játék díjazása 4 pont).

Az a játékos, aki nem tud vagy nem akar licitálni, passzol. Ha valaki passzolt, később már nem csatlakozhat a licitáláshoz.

Ahhoz, hogy valaki licitálhasson, kezében kell hogy legyen a három honőr (a skíz, a XXI-es

és a pagát) valamelyike. Akinél nincs honőr, köteles passzolni. Honőr birtokában lehetséges licitálni, de nem kötelező.

A soronkövetkező licit mindig magasabb az előzőnél, kivéve egy esetet: ha valamelyik játékos már licitált, a másik játékos magasabb licitjét módjában áll tartani ("tartom"), vagyis az előzőleg elhangzott licitet azonos értéken átvállalni. Tartani egy bizonyos licitet csak egyszer lehet: ha az utolsó licit tartom volt, vagy magasabbat kell mondani, vagy passzolni kell.

Ritkaság, hogy mind a négy játékos passzoljon. Ha ez előfordul, a kártyát összedobják, ugyanaz a játékos oszt, és a következő körben (ez négy vagy öt játszmát jelent aszerint, hányan játszanak) duplán kell fizetni ("dupla kör"). Ha a dupla körben ismét bedobják a lapot, újabb dupla kör kezdődik, így néhány parti négyszeres lesz, míg a kör vége duplán fut ki.

Ha van licitáló, a licitálás mindaddig folytatódik, mígnem három egymást követő játékos passzol, illetve a licitálást folytatni már nem lehetséges. Az utolsónak licitáló lesz a felvevő, és aszerint vesz föl a talonból három, kettő vagy egy lapot illetve semennyit, hogy mennyivel nyerte a licitet.

Léteznek konvencionális licitmenetek is, melyekben a licitáló azt ígéri, hogy egy bizonyos tarokk ill. bizonyos tarokkok nála lesznek. Ezek a konvenciók (a bridzsben használatosaktól eltérően) kötelező érvényűek: ha konvencionális jellegű licitet mond valaki, az ígért lapot ill. lapokat ténylegesen is birtokolnia kell. Részletesebb magyarázatát a kérdésnek lásd alább az invit és az engedett játék tárgyalásánál.

A szabály alól, miszerint honőr nélkül nem lehet licitálni, létezik egyetlen kivétel. Amennyiben az első három megszólaló passzolt, a negyedik játékos licitálhat, arra számítva, hogy a talonból honőrt húz fel. Ha ez nem sikerül, a játékot automatikusan elveszítette (lejátszás nincs), és az összes többi játékosnak ki kell fizetnie a partit (feltételezve, hogy a licit "három" volt, ez 1-1 pontot jelent). Ezt a licitet, tehát amikor három passz után honőr nélkül licitál a negyedik játékos, egyes helyeken próbaháromnak nevezik.

7.5. A talon felvétele és a skartolás

7.5.1. A talon kiosztása

Először a felvevő részesül a talonból, mégpedig úgy, hogy a nyerő licitnek megfelelő számú lapot kap. Ezután következik a többi játékos, az óramutató járásával ellentétes sorrendben, úgy, hogy a lapok elosztása a lehető legegyenletesebb legyen - amennyiben szükséges,

a felvevő után következő játékos plusz lapot kap:

Nyerő licit	**Felvevő**	**2. játékos**	**3. játékos**	**4. játékos**
három	3 lap	1 lap	1 lap	1 lap
kettő	2 lap	2 lap	1 lap	1 lap
egy	1 lap	2 lap	2 lap	1 lap
szóló	nem kap lapot	2 lap	2 lap	2 lap

Ha négyen játszanak, a játékosok maguk veszik fel lapjaikat (anélkül, hogy a többieknek megmutatnák azokat), ha pedig öten, az osztó osztja ki a talont, képpel lefelé.

7.5.2. A skartolás

A játékosok a talonból nyert lapokat saját kártyáik közé teszik, majd ugyanannyi lapot tesznek le, képpel lefelé. Így újból kilenc lapja lesz mindenkinek. A letett lapok neve "skart". A felvevő skartja a játékos elé kerül: ezeknek a lapoknak a pontértéke a játék végén a felvevő és partnere eredményéhez adódik. A másik három játékos által letett lapokat egyesítik: ezek öt játékos esetén az osztó elé kerülnek, ha négyen játszanak, az osztó utáni sarokra. (Ez a szokás megkönnyíti annak megjegyzését, ki a következő osztó.) Ezeknek a lapoknak a pontértékét a felvevő ellenfeleinek ütéseihez számítják (jóllehet a három skartoló egyike rendesen a felvevő partnere).

Tilos királyt vagy honőrt (tehát öt pont értékű lapot) skartolni. Invit vagy engedett játék esetén (lásd alább) ezen felül tilos még a licitben jelzett lapot fektetni. A többi lap, így a tarokkok is, szabadon lerakható.

Miután mindenki befejezte a skartolást, a skartba tett tarokkok számát - amennyiben történt tarokkfektetés - be kell jelenteni. Ha öten játszanak, a felvevőtől különböző három játékos skartját az osztó nézi meg, majd jelentést tesz: "tiszta", amennyiben nincs tarokk a lapok közt, ill. "egy tarokk fekszik", "két tarokk fekszik" stb. Ha csak négyen játszanak, az osztó is részt vesz a partiban, így nem nézhet bele a skartba. Ezért ebben az esetben a skartolás befejeztével a tarokkot fektető játékos maga jelenti be az általa skartolt tarokkok számát. "Tiszta" bejelentést senki nem tesz, ha nem skartolt tarokkot: a csendben maradó játékosról tudhatni, hogy kizárólag színt fektetett.

Amennyiben a felvevő skartol egy vagy több tarokkot, miután mindenki letett, fölüti az illető lapot ill. lapokat, így a többi játékos nemcsak arról értesül, hány tarokkot tett le, hanem arról is, melyek ezek a kártyák. A skartolt tarokkot ill. tarokkokat a felvevő az első lap kihívásáig hagyja fölütve.

7.5.3. A játék eldobása

Néhány különösen gyenge lapösszeállítás följogosítja a játékost, hogy a partit semmissé nyilvánítsa. Ezek a lapok a következők:

- mind a négy király
- a XXI-es mint egyetlen tarokk
- a pagát (I) mint egyetlen tarokk
- kilenc színes lap
- a XXI-es és a pagát, valamint hét színes lap

A játék semmissé tétele nem kötelező - a fenti lapok bármelyikének birtokában dönthet úgy a játékos, hogy mégis játszik, amennyiben ennek értelmét látja. Az első eset kivételével nincs megengedve a játék semmissé tétele, ha a skartba a játékos tarokkot tett. Négy királlyal tarokkfektetés után is el lehet dobni a lapot. A játék semmissé nyilvánítására kizárólag a lapcsere után van lehetőség: ha elkezdődtek a bemondások, már késő.
Nem feltétlenül kézenfekvő, hogy az egy kézben lévő négy király gyenge lap. A királyok voltaképpen felelősséget jelentenek: öt pontot érnek, szinte mindig megütik őket, skartba viszont nem tehetőek.
Ha a játékot valaki semmissé nyilvánítja, nincs díjazás. A lapot bedobják, az osztó újra oszt, és a következő négy ill. öt partit (aszerint, hogy hányan játszanak) duplán írják, ahhoz hasonlóan, mint amikor négy passzt követően nincs játék.

7.6. Partnerhívás, figurák, egyéb bemondások

A játéknak a lapcsere befejezése után következő szakasza némileg hasonlít a licitáláshoz. Ezúttal a felvevő szól először, majd a többi játékos következik az óramutató járásával ellentétesen haladva, akár több körön át. A bemondások négy csoportba sorolhatók:

1. Ha valamelyik játékosnak nyolc vagy kilenc tarokkja van, ezt bejelentheti
2. A felvevő partnert hív
3. A játékosok bármelyike bemondhat egy vagy több figurát
4. A játékosok bármelyike kontrázhatja, rekontrázhatja stb. a játékot ill. az ellenfél által korábban bemondott figurákat

Ezeket a későbbiekben részletesen tárgyaljuk: ekkor kerül sor a bemondások menetének magyarázatára is.

7.6.1. Partnerhívás

A bemondásokat a felvevő kezdi azzal, hogy partnert hív. A szóbanforgó játszmában a meghívott tarokk birtokosa lesz a felvevő partnere (segítője). A másik két játékos alkotja az ellenpártot (ellenfelek, ellenjátékosok vagy védők). A felvevő ezekkel a szavakkal hív partnert: "Hívom a húszast" vagy "Segít a húszas". A XX-as kötelező meghívásától a következő három esetben lehetséges eltérni:

1. Ha a XX-as magánál a felvevőnél van, azt a XX-as alatti legmagasabb tarokkot hívhatja, amelyik nincs a kezében. Például a skíz, XX, XIX, XVIII, XV, XIII, VII tarokkok birtokában lehetséges a XVII-es meghívása. Ugyanakkor a felvevő meghívhatja saját XX-asát is, mely esetben egyedül játszik a mások három játékos alkotta ellenpárt ellen, jóllehet amazok ezt csak később fogják felismerni.

2. Ha a másik három játékos valamelyike tarokkot skartolt, a felvevő bármely - honőrtől különböző - tarokk partnerül hívására jogosult. Ha éppen a skartba tett tarokkot hívja meg, egyedül játszik három ellenében. Ebben az esetben a meghívott tarokkot fektető játékos köteles megkontrázni a játékot (lásd alább).

3. Ha a másik három játékos valamelyike invitet adott, amelyet a felvevő elfogadott (lásd alább), a felvevő nem hívhatja a XXast: helyette az invit során jelzett lapot (a XIX-est ill. a XVIII-ast) kell meghívnia. Engedett játék esetén a felvevő köteles a XX-ast hívni, még akkor is, ha tarokkfektetés történt - a jelzett tarokkot nem lehet elskartolni, és kötelező meghívni.

A meghívott tarokk birtokosa lesz a felvevő partnere, ám ezt semmilyen módon nem árulhatja el. Kiléte csak a következőkben - tehát a bemondások és a lejátszás során - derül ki. Néha az együtt játszók személye egészen a partnerül hívott tarokk kijátszásáig rejtély marad.

7.6.2. A figurák

A játék során bizonyos figurák teljesíthetők, amelyek külön díjazásban részesülnek. A figurákat az együtt játszók közösen teljesítik ill. bukják el: ha valamelyik játékos pagátultimót csinál, vagy XXI-esét elveszíti az ellenfél skízével szemben, partnere ugyanannyit nyer ill.

veszít, mint ő. Ha a játékos úgy gondolja, hogy valamelyik figurát teljesíteni tudja, a lejátszást megelőző bemondások során ezt a szándékát előre bejelentheti. Amennyiben a figura sikerül, partnerével együtt kétszeres díjazásban részesül, ha azonban nem, a veszteség is kétszeres. A figurák díjazása - akár "csendben", akár "bemondva" - általában egymástól független: miközben az egyik sikerül, a másik elbukhat. (Kivétel a duplajáték és a volát, amelyek hatással vannak egymásra ill. a díjazásra - lásd alább az elszámolás fejezetben.)
A Paskievics-tarokkban hat figura van:

1. Tulétroá, röviden tuli, trull vagy trúl. Neve a francia "tous les trois" ("mind a három") kifejezésből származik, jelentése, hogy a partnerek mind a három honőrt (a skízt, a XXI-est és az I-est, vagyis a pagátot) hazaviszik ütéseikben. Díjazása: 1 pont csendben, 2 pont bemondva.

2. Négykirály. Jelentése: a partnerek mind a négy királyt hazaviszik ütéseikben. Díjazása: 1 pont csendben, 2 pont bemondva.

3. Duplajáték. Jelentése: a partnerek ütéseikben hazaviszik a lapok összpontértékének háromnegyedét, vagyis legalább 71 pontot, miközben az ellenfél pontjainak száma értelemszerűen nem haladja meg a 23at. A figura díjazása úgy történik, hogy csendes teljesítés esetén a játék megnyeréséért járó pontokat megkétszerezik, ha pedig a duplajáték be lett mondva, megnégyszerezik.

4. Volát. Jelentése: a partnerek mind a kilenc ütést hazaviszik. Díjazása csendben a játék megnyeréséért járó pontok háromszorosa, bemondva hatszorosa.

5. Pagátultimó, másként pagátulti. Jelentése: az utolsó ütés a pagáttal (az Ies tarokkal) történik. A csendes pagátulti díjazása 5 pont. Sikeréhez az szükséges, hogy kilencedikre maga a pagát üssön. Amennyiben a pagátot kilencedikre játsszák ki, de azt egy másik tarokkal leütik, a pagátulti elbukott, és a partnerek 5 pontot fizetnek a másik oldalnak ("pagátulti-fogás"). Ez még akkor is így van, ha az ultit a pagátos partnere "fogta el". Ha bemondták, a figura díjazása 10 pont. A bemondott pagátultimó három módon bukhat el: a pagátot az utolsó ütésben leüti egy tarokk; birtokosa a pagátot kijátszani kényszerül a kilencedik ütés előtt; a pagát nincs is a bemondóknál (ritka).

6. Huszonegyfogás. Jelentése: a skíz leüti, "elfogja" az ellenfél XXI-esét. Díjazása: 21 pont. Nem számít XXI fogásnak, így nincs is díjazva, ha a skíz és a XXI-es partnerek,

és a két lap azonos ütésbe esik. A bemondott XXI fogás jutalma 42 pont; ha a XXI-es megszökik, vagy nem is volt az ellenfeleknél, a bemondók fizetik a 42 pontot.

7.6.3. Kontrázás

A bemondások során a felvevő ellenfele megkétszerezheti a játék díjazását, amennyiben "kontra játék"-ot mond. Hasonló módon kontrázhatja a többi figurát is a figura bemondójának ellenfele, így duplázva meg díjazásukat. A kontrák egymástól függetlenek, ezért a játékosnak meg kell mondania, melyik figurát kontrázza, pl. "kontra pagátultimó" vagy "kontra játék és négykirály". Ha a játékot ill. valamelyik bemondást megkontrázták, a bemondó vagy partnere "rekontrázhat", a díjazást újból megduplázva. Elméletben a kontrák (és a duplázás) tovább folytathatók: a rekontra után "szubkontra", "hirskontra" és "mordkontra" következhet. "Egyes játék" esetében például, ahol a játék alapdíja 3 pont, kontrázva 6, rekontrával 12, szubkontrával 24, hirskontrával 48, mordkontrával pedig 96 pont fizetendő. Szubkontránál magasabb kontra a gyakorlatban igen ritka.

7.6.4. A tarokkszám bemondása

Az a játékos, akinek nyolc vagy kilenc tarokkja van, ezt a bemondások során bejelentheti ("nyolc tarokk", "kilenc tarokk"). A nyolc ill. kilenc tarokkot a másik három játékos azonnal fizeti: nyolc tarokkért 1-1 pont, kilencért 2-2 pont jár. A tarokkszám bejelentése nem kötelező. Kivétel ez alól a pagátultimó bemondója ill. a pagátultit megkontrázó játékos, aki köteles bejelenteni, ha nyolc vagy kilenc tarokkja van.
Kilenc tarokkal nyolc tarokkot mondani nem szabad.
Ha a játékos nyolc ill. kilenc tarokkját nem jelentette be a bemondások során, a lejátszás után igényelheti annak díjazását, de ilyenkor már csak partnerétől, tehát az ellenfelektől nem. Ezt az igényt csak akkor illik benyújtani, ha az illető párt a játszmát olyan nyereséggel zárta, amelyből a díjazás fedezhető.

7.6.5. A bemondások menete

Először a felvevő beszél. Amennyiben van tarokkszáma, azt bemondhatja, utána partnert hív, ezt követően bemondja a kívánt figurákat, végül "passz"-szal vagy "mehet"-tel jelzi, hogy befejezte a beszédet. Tehát először a tarokkszám, utána a partnerhívás, majd a figurák bemondása tetszőleges sorrendben. Egy meglehetősen erős lappal rendelkező felvevő lehetséges bemondása például: "Nyolc tarokk, hívom a tizenkilencest, tulétroá, négykirály,

passz".

A játéknak ez a szakasza, tehát a bemondások folytatódnak az óramutató járásával ellentétes irányban. A soron következő játékos tarokkszámot mondhat, figurát mondhat be, ill. az ellenfél által korábban bemondott figurákat kontrázhatja. A bemondások minden esetben passzal zárulnak, minekutána a következő játékosé a szó. A bemondások mindaddig folytatódnak az asztal körül, mígnem három egymást követő játékos passzol.

Bármely játékos bemondhat bármilyen figurát, és ezekért a bemondásokért a bemondó és partnere együttesen áll helyt. Így például, ha a játékos arra a következtetésre jut, hogy partnerénél van a pagát, ő is bemondhatja a pagátultimót, arra kötelezve játékostársát, hogy a pagáttal vigye haza az utolsó ütést. A duplajáték és volát bemondásával kapcsolatban van néhány megszorítás:

1. A duplajátékot és a volátot nem lehet egyugyanazon alkalommal bemondani.

2. Ha a volát már elhangzott, nem lehet duplajátékot mondani.

Amikor a játékos bemond egy figurát, szükséges tudni, melyik oldal nevében beszél, másszóval hogy a felvevővel van vagy ellene. Ha ez nem így lenne, lehetetlenné válnék kontrázni ezeket a bemondásokat, hiszen nem lehetne tudni, a bemondó a kontrázni kívánónak partnere vagy pedig ellenfele. A helyzet tisztázása a következőképpen történik:

- Ha a játékos bemond valamit, és más úton nem tudható, kivel van, úgy kell tekinteni, hogy az utoljára szóló (bemondó ill. kontrázó) játékos partnere. Ha figura még nem lett bemondva ill. kontrázva, a beszélő a felvevő partnere.

- Ebből következik, hogy az a játékos, aki be akar mondani valamit, de előtte valamelyik ellenfele beszélt (ill. ha a szóbanforgó játékos a felvevő ellenfele, és a felvevőn kívül senki nem beszélt még), köteles megkontrázni (adott esetben rekontrázni) valamit, amit az ellenpárt mondott be, így téve világossá, melyik oldal nevében beszél.

- Ha már ismert, hogy a játékos melyik oldalon áll - akár a licitből (tehát engedett játék vagy invit volt), akár a korábbi bemondásokból, vagy pedig azáltal, hogy maga a játékos tette azt világossá korábbi bemondásával -, már nem szükséges kontrával jelezni a hovatartozást.

A fenti szabályok nem vonatkoznak a tarokkszám bemondására. A nyolc ill. kilenc tarokk bemondása simán történik, így a játékosok nem is tudják feltétlenül, kivel van a bemondó. Értelemszerűen a csak tarokkszámot bemondó játékos után beszélő sincs feltétlenül egy oldalon az illető játékossal.

7.7. A lejátszás

A bemondások végeztével kezdetét veszi a lejátszás. Az osztó után következő játékos hív először, az első ütés elvivője másodszor, és így tovább. Hívni bármelyik lapot lehet, a többi játékos köteles a hívott színre ugyanolyan színt, tarokkra tarokkot tenni.

Ha a hívott színből valakinek nincsen, tarokkot kell tennie. Csak ha sem megfelelő színe, sem tarokkja nincsen, tehet a játékos bármilyen lapot az ütésbe. Az ütést a benne szereplő legmagasabb tarokk viszi el, ha pedig nincs benne tarokk, a hívott szín legmagasabb lapja.

Ha pagátultimó-mondás történt, a pagát birtokosa köteles az utolsó pillanatig megőrizni pagátját, magyarán nem játszhatja ki mindaddig, amíg rá nem kényszerül a fenti szabályok értelmében, miszerint színre színt kell tenni, ha pedig nincs, tarokkot. Korábban kijátszani a pagátot tehát akkor sem szabad, ha világos, hogy nem fog ütni kilencedikre.

Mivel a lejátszás kezdeti szakaszában gyakran nem tudható, ki kivel van, a játékosok saját - képpel lefelé fordított - ütéseiket külön gyűjtik, és az ellenjátékosok skartja is külön tartandó. Csak amikor a meghívott tarokkot kijátsszák, vagy más bizonyító erejű esemény történik, amelyből tudható, kik a partnerek, lehet az ütéseket ill. a skartot egyesíteni páronként.

Ha mind a kilenc ütés lezajlott, az ütésekben rejlő pontokat megszámolják, és a játszmát fizetik. Ezután az utolsó osztótól jobbra ülő játékos kever, emeltet és oszt a következő partihoz.

7.7.1. Az elszámolás

Az elszámolás rendszere azon alapul, hogy a játékosok minden egyes parti befejezése után pénzzel fizetnek egymásnak. Ha a játszma során ketten-ketten játszanak egymás ellen, a vesztes játékosok egyike ill. másika kifizeti a nyertesek egyikének ill. másikának a játék valamint a megjátszott figurák díjának végösszegét. Ha valaki egyedül játszik három ellen (minthogy magát hívta meg, vagy pedig egy elskartolt tarokkot), a végösszeget mindhárom játékostól megkapja (ill. ha vesztett, mindháromnak fizeti), így a felvevő ez esetben háromszoros értéken nyer ill. veszít. Ha öten játszanak, az elszámolás csak a négy ténylegesen játszót érinti: az osztó nem nyer és nem is veszít. Ha az eredményt papíron vezetik, a nyereséget pluszként, a veszteséget mínuszként jegyzik, így a játékosok pontjainak végösszege mindig nulla.

Először a játékostársak által ütött pontokat számolják meg a fentebb ismertetett lapértékeknek megfelelően. A lapok összértéke 94 pont. Ha a felvevő és társa eléri a 48 pontot

(vagyis a pontok több mint felét), megnyerte a játékot. Az ellenfél akkor nyer, ha legalább 47 pontot ütött. Ha valamelyik oldal a pontok több mint háromnegyedét hazaviszi, vagyis a másik félnek legfeljebb 23 pontja marad, duplajátékról van szó. Ha valamelyik oldal minden ütést elvitt, volátot csinált.

A játék alapdíját a nyertes licit határozza meg. Háromtól szólóig a játék alapdíja egyesével nő 1-től 4-ig. Duplajáték esetén az alapdíj kétszeresét, volát esetén az alapdíj háromszorosát számolják el. Ha a duplajátékot bemondták, a szorzó négyszeres, ha pedig bemondott volát volt, hatszoros.

Fontos megjegyezni, hogy amennyiben kontrák nem voltak, a játék, a duplajáték és a volát díjazása vagylagos: ha például kettes játékban a felvevő és partnere 75 pontot üt, a duplajátékért járó 4 pont a sima játék 2 pontjának helyébe lép, nem pedig hozzáadódik.

Ha a duplajátékot ill. a volátot bemondják, vagy ha a játékot megkontrázzák, a helyzet bonyolultabb. A játék, duplajáték és volát díjazását meghatározó szabályok a következők:

1. Ha sem duplajátékot sem volátot nem mondtak, és a játék sem lett megkontrázva, akkor a játék, a duplajáték és a volát közül csak egy részesül díjazásban, az elért pontok ill. ütések függvényében.

2. Ha valamelyik fél bemondja a duplajátékot, a sima játékért már nem kap semmit, ám a volátért még írhat pontot, amennyiben valamennyi ütést elviszi. Ha viszont nemcsak a duplajátékot, de a partit is elbukja, az ellenfél nemcsak a duplajáték díját kapja meg, hanem a sima játékért járó pontot ill. pontokat is (összesen tehát a játék alapértékének ötszörösét). Ha ráadásul az ellenfél maga csinál duplajátékot, netalán volátot, a sima játék helyett azt írja, természetesen a bemondott és elbukott duplajátékon felül.

3. Ha valamelyik oldal mind a duplajátékot mind a volátot bemondja, akkor mindkét figurát díjazzák: lehetséges megnyerni a duplajátékot, miközben a volát elbukik. Ekkor a sima játékot nem számolják, kivéve ha a bemondó fél elbukja azt, mely esetben az ellenfél írja az érte járó pontokat. Abban a kevéssé valószínű esetben, ha az ellenfél ezek után csendes duplajátékot vagy volátot ér el, a sima játék helyett azt írja.

4. Ha valamelyik fél a volátot anélkül mondja be, hogy duplajátékot mondana, a volátot fizetik (akár sikerül, akár nem). A bemondó sem a sima játékért sem a duplajátékért nem kap pontot, ha azonban az ellenfél nyeri a játékot (netán duplajátékot vagy volátot csinál), díjazásban részesül érte.

5. Ha a játékot megkontrázzák, minden körülmények között díjazás jár érte. Ha valamelyik oldal csendes duplajátékot vagy volátot ér el, a kontrázott játékon felül ír érte pontokat (de csendes volát esetében a csendes duplajátékért nem).

6. Ha a játékot kontrázzák (ill. rekontrázzák), és a duplajátékot és/vagy a volátot valamelyik oldal bemondja, nemcsak a bemondott figurák, hanem a játék is díjazásban részesül. A kontrázott játékon és bemondott duplajátékon felül lehetséges csendes volátot írni.

A fenti bemondások mindegyike mindkét oldal rendelkezésére áll. Lehetséges, hogy valamelyik figurát az egyik fél kétszer írja: pl. ha bemondják a négykirályt, de az ellenfél viszi el mind a négy királyt, az illető játékosok 3 pontot kapnak - kettőt a bukott figuráért és további egyet saját csendes négykirályukért. Még az is elképzelhető, hogy ugyanazt a figurát mindkét oldal bemondja: például az A csapat bemondja a négykirályt, amelyet a B csapat megkontráz, és ráadásul maga mondja be a négykirályt. Ebben az esetben, ha valamelyik fél ténylegesen teljesíti a négykirályt, 6 pontot kap, ha a királyokból mindkét oldalnak jut, mindkét bemondás elbukik, és a két bemondás díjának összegzése nyomán a B csapat kap 2 pontot.
Az a szabály, miszerint volát esetében csendes trull és négykirály nem számolható el, érdekes következménnyel jár. Ha hármas a játék, és semmi sincs bemondva, az összes honőr és király elvitele esetén jobban jár a játékos, ha egy ütést kienged, s így duplajátékot, trullt és négykirályt csinál 4 pontért (2 + 1 + 1), mintha minden ütést elvisz, tehát volátot játszik, amely csak 3 pontot ér.

7.8. Konvencionális licit: invit és engedett játék

A konvencionális licit célja az, hogy a két nagyhonőrös, ha erős lapja van, még akkor is egymással lehessen, ha egyiküknél sincs a XX-as. Ennek révén mód nyílik értékes figurák bemondására és teljesítésére.

7.8.1. Invit

Az invit arról szól, hogy az invitet adónál van egy meghatározott tarokk - a XIXes vagy a XVIIIas. Az invitadó tehát arra törekszik, hogy a licit nyertesét partnerévé tegye, mégpedig úgy, hogy amaz felvevőként az őáltala jelzett tarokkot hívja meg.
Ehhez hasonló konvenciók a bridzsben is vannak, ám lényeges különbség, hogy a bridzstől

eltérően a tarokkban az invit a szorosan vett szabályok közé tartozik. Nem szabad invitet adni ill. engedni a játékot, ha a jelzett tarokk nincs a játékosnál. Másfelől akkor sem kötelező invitet adni ill. engedni a játékot, ha az ahhoz szükséges lap a játékos kezében van - éppúgy lehetséges passzolni, vagy rendesen licitálni.
Az invitadás a licitmenetben történő ugrással jön létre:

- a soronkövetkező rendes licithez képest történő egy lépés ugrás invit a XIX-esre (vö. játékváltozatok)
- a soronkövetkező rendes licithez képest történő két lépés ugrás invit a XVIIIasra

Ha a licitet az invitet adótól különböző játékos nyeri meg, a felvevő köteles az invitben jelzett tarokkot hívni partnerül.
Két olyan helyzet képzelhető el, amikor a licitben történő ugrás nem invit:

1. Egy licitálás során csak egy invit lehetséges. Ha tehát valamelyik játékos már invitet adott, a licitálásban történt újabb ugrásnak nincs konvencionális jelentése.
2. Ha az első három licitáló passzol, a negyedikként megszólaló játékos licitje semmiképpen sem tekinthető invitnek. Ebben a helyzetben nem is lenne sok értelme invitet adni, hisz egyik játékos sincs abban a helyzetben, hogy fogadja, és a jelzett lapot hívja partnerül.

Az invitet adó játékostól rendszerint elvárható, hogy erős lapja és nagyhonőrje legyen. Invitet adni pagáttal is lehetséges, ám ebben az esetben van egy további megszorítás: a partnerhívás után az első adandó alkalommal pagátultimót kell mondania a játékosnak ("kötelező pagátulti-mondás").

7.8.2. Engedett játék

A konvencionális licitálás másik módja az úgynevezett engedett játék. Ez egyféleképpen történhet: valamelyik játékos hármat mond, egy másik erre kettőt, miközben a maradék két játékos passzol. Ekkor az elsőnek hárommal licitáló passzol ("elpasszolja a kettőt"). Ennek konvencionális jelentése van, mégpedig az, hogy a passzoló játékosnál van a XXas, valamint legalább az egyik nagyhonőr (a skíz vagy a XXI-es).

Irodalomjegyzék

[BCR86] Gilles Brassard, Claude Crepeau, and Jean-Marc Robert. All-or-nothing disclosure of secrets. *Advances in Cryptology – CRYPTO '86 LNCS*, 263:234–238, 1986.

[BS03] Adam Barnett and Nigel P. Smart. Mental poker revisited. *Cryptography and Coding 2003, LNCS 2898*, pages 370–383, 2003.

[BV04] Levente Buttyán and István Vajda. *Kriptográfia és alkalmazásai*. Typotex Kiadó, 2004.

[CDS94] Ronald Cramer, Ivan Damgard, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. *Advances in Cryptology – CRYPTO '94 LNCS 2898*, 839:174–187, 1994.

[CP93] David Chaum and Torben Pryds Pedersen. Wallet databases with observers. *Advances in Cryptology – CRYPTO '92, LNCS 740*, pages 89–105, 1993.

[CR05] Jordi Castellá-Roca. *Contributions to Mental Poker*. PhD thesis, Universitat Autonóma De Barcelona, 2005.

[Cre87] Claude Crepeau. A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or how to achieve an electronic poker face. *Crypto '86*, pages 239–247, 1987.

[ElG85] Taher ElGamal. A public key cryptosystem and a signature scheme on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.

[FS90] Uriel Feige and Adi Shamir. Witness indistinguishable and witness hiding protocols. *STOC*, 839:416–426, 1990.

[GK03] Shafi Goldwasser and Yael Tauman Kalai. On the (in)security of the fiat-shamir paradigm. *In FOCS, IEEE Computer Society*, pages 102–, 2003.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences, LNCS 2898*, 28(2):270–399, 1984.

[Gol05] Philippe Golle. Dealing cards in poker games. *In Proceedings of the International Conference on Information Technology: Coding and Computing*, pages 506–511, 2005.

[MvOV96] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[Ped91] Torben Pryds Pedersen. A threshold cryptosystem without a trusted party. *In Eurocrypt '91, LNCS*, 547:522–526, 1991.

[PS00] David Pointcheval and Jacques Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13(3):361–396, 2000.

[Sch98] Christian Schindelhauer. A toolbox for mental card games. Technical report, Medizinische Universität Lübeck, 1998.

[Sta05] Heiko Stamer. Efficient electronic gambling: An extended implemetation of the toolbox for mental card games. *WEWoRC 2005. LNI P-74*, pages 1–12, 2005.