Abandono de jugadores en esquemas distribuidos de juego de cartas *

Jordi Castellà-Roca, Francesc Sebé y Josep Domingo-Ferrer

Dept. d'Enginyeria Informàtica i Matemàtiques,
Universitat Rovira i Virgili,
Av. Països Catalans 26, E-43007 Tarragona
e-mail {jcaste,fsebe,jdomingo}@etse.urv.es

Resumen En la literatura existe multitud de propuestas de esquemas para juegos de cartas distribuidos a través de redes de comunicaciones (conocidos como esquemas de *mental poker*). En dichos esquemas es preferible que no exista la necesidad de intervención de una Tercera Parte de Confianza (TPC) o que su participación sea mínima. En este artículo estudiamos el problema del abandono de jugadores en diversas propuestas de esquemas sin TPC. A continuación proponemos una solución *optimística* a dicho problema. Una solución optimística es aquella en que se añade una TPC al esquema pero que solamente interviene en aquellos casos en que alguno de los jugadores no sigue el esquema de forma correcta.
Palabras clave: Mental poker, Tercera Parte de Confianza.

1. Introducción

El *mental poker* se juega como el juego tradicional de cartas pero sin la necesidad de que los jugadores se encuentren físicamente en un mismo lugar y comunicándose íntegramente a través de una red de comunicaciones. En esta situación, cualquier jugador puede actuar de forma deshonesta e intentar hacer trampas.

Un esquema de mental poker debe ofrecer todos los protocolos necesarios que permitan jugar una partida. Éstos son: mezcla de cartas, extracción de una carta de la baraja, desechar una carta y mostrar una carta.

Dichos protocolos deberían garantizar las mismas propiedades de seguridad que se dan en un partida tradicional más las que se derivan de la propia condición del juego electrónico. Estas propiedades fueron enumeradas por Crépeau [8].

* Este trabajo ha sido parcialmente financiado por el Ministerio Español de Ciencia y Tecnología y el fondo FEDER bajo el proyecto "STREAMOBILE" (TIC-2001-0633-C03-01).

- Unicidad de las cartas
- Distribución uniforme de las cartas mezcladas
- Alta probabilidad de detección de jugadores deshonestos
- Confidencialidad de las cartas
- Minimización del efecto de las confabulaciones de jugadores
- Completa confidencialidad de la estrategia
- Ausencia de una Tercera Parte de Confianza (TPC).

En los aspectos prácticos se debe añadir otra propiedad: tolerancia al abandono de jugadores. En cualquier juego remoto se puede dar el caso que un jugador deje de participar. El abandono puede ser:

- **Intencionado:** es el jugador quien decide abandonar el juego. Un ejemplo sería el caso de jugadores a quienes la partida es desfavorable y deciden no continuar.
- **No intencionado:** el jugador no puede continuar en el juego. Por ejemplo, a causa de un corte en las comunicaciones.

No es tolerable que en caso de abandono por parte de uno de los jugadores la partida se deba interrumpir. En estos casos el resto de jugadores debería poder continuar.

1.1. Estructura del artículo

Nuestro trabajo se estructura de la siguiente forma. La sección 2 presenta una descripción de las distintas propuestas de esquemas de mental poker presentes en la literatura. Las distintas propuestas se exponen clasificadas según utilicen o no una TPC y teniendo en cuenta si la estrategia de los jugadores se mantiene en secreto al término de cada partida.

A continuación, la sección 3, contiene una clasificación de las TPC basada en el grado de implicación en los protocolos donde participan.

En la sección 4 se detalla nuestra propuesta *optimística* que permite que los esquemas más avanzados de mental poker ofrezcan tolerancia al abandono de jugadores.

Finalmente, la sección 5 detalla las conclusiones y el trabajo futuro.

2. Propuestas actuales de esquemas de mental poker

A continuación presentamos un resumen de diferentes propuestas de esquemas de mental poker existentes en la literatura.

2.1. Esquemas basados en TPC

Algunos autores ofrecen las propiedades enumeradas por Crépeau mediante el uso de una Tercera Parte de Confianza (TPC). Estos autores argumentan que el uso de la TPC es necesario por la necesidad de eficiencia o simplemente por la dificultad de cumplir con todas las propiedades enumeradas.

Podemos dividir las principales propuestas que utilizan TPC según las partes del juego en que participa.

En [6], la TPC realiza todas las acciones del juego, es decir, la mezcla de las cartas y el reparto a los jugadores.

En [13,24] los jugadores y la TPC realizan conjuntamente la mezcla de cartas, mientras que reparto lo realiza íntegramente la TPC.

En el trabajo [11] se propone un esquema en el que la TPC solamente participa en la mezcla de la baraja. El reparto de cartas se hace de forma colaborativa entre los jugadores.

2.2. Esquemas sin TPC con revelación de estrategia

Algunos autores argumentan que la utilización de una TPC en la mezcla o reparto de las cartas no garantiza un juego honesto porque en condiciones reales puede ser manipulada. La TPC, en definitiva, será una entidad de un sistema controlado por un administrador. La confabulación de éste con algun jugador puede perjudicar al resto.

El primer esquema de mental poker sin TPC [20] únicamente permitía el juego entre dos jugadores. Posteriormente, en [17,7] se demostró que el criptoesquema utilizado filtraba cierta información, concretamente un bit, de las cartas. En [14] se presentó una solución a dicho problema.

En [12] se presenta una propuesta segura para juegos con dos jugadores.

En los trabajos [1,23] se permite que más de dos jugadores participen en el juego. Sin embargo no son resistentes a confabulaciones, es decir, si dos jugadores se confabulan pueden conocer las cartas del resto de jugadores.

El esquema [25] es eficiente y permite que varios jugadores participen en el juego. Sin embargo, en [5] se demuestra que dicho protocolo es inseguro al presentar una debilidad que permite que un jugador cualquiera pueda descifrar las cartas sin conocer la información secreta del resto de jugadores.

Las propuestas [8,4] presentan sendos esquemas para varios jugadores resistentes a confabulaciones.

Todos los esquemas descritos en esta sección requieren que al finalizar la partida, cada jugador revele su información secreta para permitir verificar que ha ejecutado correctamente todos los protocolos. Tal como se ha dicho anteriormente, este hecho permite que se conozcan las decisiones tomadas por los jugadores, es decir, su estrategia.

2.3. Esquemas sin TPC y sin revelación de estrategia

Los esquemas descritos en esta sección cumplen todos los requisitos enumerados por Crépeau. Sin embargo, para que sean utilizables en la práctica es necesario que contemplen el problema del abandono de jugadores. Vamos a describirlos desde este punto de vista.

Los esquemas [9,21] no contemplan el abandono de jugadores. En estas propuestas cada jugador dispone de cierta información secreta necesaria para extraer cartas de la baraja. Sin esta información no es posible continuar con la partida.

El esquema descrito en [2] propone como solución al problema que los jugadores que abandonan el juego entreguen su información secreta. Sin embargo esta solución solamente es aplicable en el caso de abandono intencionado de un jugador. Si el abandono se produce, por ejemplo, por un corte en las comunicaciones, esta entrega no se podrá realizar.

Las propuestas de [15,16,22] también satisfacen las propiedades de Crépeau. En estas propuestas cada una de las cartas de la baraja está representada por un valor distinto. En la mezcla de las cartas, los valores son cifrados y permutados por cada uno de los jugadores. El efecto de cifrar es el equivalente a girar las cartas en una baraja tradicional. En este proceso se utiliza un esquema de compartición de secretos, de manera que se define un umbral mínimo de jugadores necesario para descifrar los valores. El objetivo es permitir que el juego continue si un jugador abandona el juego.

El esquema de compartición en [15,16] se aplica a las cartas. Cada valor que representa una carta es dividido en tantas partes como jugadores, y cada una de las partes se cifra con la clave pública de un jugador distinto. Para descifrar una carta es necesaria la participación de un número de jugadores igual o superior al umbral. En [22] los jugadores crean un par de claves de acuerdo con el esquema propuesto en [19]. Los jugadores generan una clave pública de manera que cada jugador tiene una parte de la clave privada, y para utilitzar la clave privada es necesario que participe un número mínimo de jugadores fijado en el protocolo, el umbral.

En el caso de abandono por parte de algún jugador, la partida podrá continuar simpre que el número de jugadores restantes sea superior a dicho umbral. Sin embargo la utilización de un esquema de compartición de secretos permite que una confabulación lo bastante numerosa de jugadores pueda obtener toda la información de la baraja.

Por consiguiente, podemos afirmar que el hecho de permitir el abandono de jugadores mediante la utilización de un esquema de compartición sobre la clave secreta abre la posibilidad de que se produzcan confabulaciones que permitan conocer el valor de las cartas. En este caso, para conseguir una propiedad se pierde otra.

3. Clasificación de las TPC

El diseño de protocolos para su ejecución por parte de participantes que no confían entre sí es un tema complejo.

Un protocolo es *justo* cuando ninguno de sus participantes puede quedar con ventaja respecto a los demás a causa de una ejecución con parámetros incorrectos o a una interrupción de la misma.

Existe multitud de situaciones donde se requiere un protocolo justo. Algunos ejemplos son: la firma distribuida de contratos [3], la venta electrónica de productos con pago [18], el correo electrónico certificado [10] y el mental poker.

En la literatura existe multitud de propuestas de protocolos justos basados en una Tercera Parte de Confianza (TPC). Estos protocolos se basan en añadir un participante al protocolo en quien el resto de jugadores confía. Esta confianza se basa en la suposición de que la TPC ejecutará correctamente todos los pasos del protocolo en que interviene y que no revelará información confidencial a la que tenga acceso.

Según el grado de implicación de la TPC en el protocolo, éstas se pueden dividir en:

- **TPC activas:** La TPC participa activamente en cada ejecución del protocolo.
- **TPC secundarias:** La TPC solamente interviene en caso de que haya una ejecución anormal. Los protocolos que las utilizan se denominan *optimísticos*.

4. Propuesta contra el abandono de jugadores basada en una TPC secundaria

En la sección 2.3 se ha enumerado un conjunto de esquemas propuestos en la literatura que cumplen todas las propiedades enumeradas por

Crépeau. Sin embargo, su utilización práctica se ve seriamente limitada por su falta de tolerancia al problema del abandono de jugadores.

A continuación proponemos una solución que permite dotar dichos esquemas con la propiedad de tolerancia al abandono de jugadores mediante la inclusión de una TPC secundaria.

4.1. Nuestra propuesta

En nuestra propuesta, se añade una TPC a quien, al inicio de la partida, los jugadores confían la custodia la información secreta que utilizarán durante la partida. Esta TPC únicamente participará en el juego en el caso que alguno de los jugadores abandone.

Cuando un jugador abandona, la TPC toma parte en el juego realizando las operaciones necesarias para que el resto de jugadores pueda continuar. Esta condición determina el grado de implicación de la TPC. Según este grado de implicación, realizamos la siguiente clasificación.

Esquemas que permiten una participación puntual En los esquemas [15,16,22,2] para destapar una carta es necesario que cada uno de los jugadores intervenga. Si uno de ellos abandona, la partida no puede seguir.

En estos esquemas, en el caso que un jugador abandone, la TPC utiliza la clave secreta de éste que tiene en custodia para descifrar su parte de las cartas que quedan en la baraja. De esta forma el resto de jugadores podrá continuar jugando. Después, ya no será necesaria ninguna otra intervención por parte de la TPC.

Esquemas que requieren una participación activa En el esquema de [9] cada uno de los n jugadores dispone de una permutación de 52 elementos (recordemos que una baraja de poker tiene 52 cartas), y la baraja está formada por la composición en un cierto orden establecido de estas permutaciones. Una carta es el resultado de permutar un valor comprendido entre 1 y 52 por la composición de las n permutaciones. Las permutaciones de los jugadores no son públicas. Cada jugador guarda su permutación en secreto.

En este protocolo, la publicación de la permutación de un jugador que ha abandonado la partida, permitiría a algunos de los jugadores restantes obtener información sobre las cartas que extrajo. De esta manera se filtraría información sobre las cartas que quedan en la baraja.

Por este motivo, la única forma de continuar con la partida es que la TPC participe en las siguientes extracciones de cartas ocupando el puesto del jugador que ha abandonado. Esto significa que la TPC participará de forma activa durante el resto del juego.

4.2. Protocolo de custodia de información secreta

Tal como hemos expuesto en la sección 4.1, antes de comenzar una partida, la TPC adquiere la custodia de la información secreta de cada jugador. A continuación presentamos un protocolo mediante el cual los jugadores entregan su información a la TPC.

La TPC y los jugadores deben disponer de un par de claves pública-privada (P_k, S_k).

En el inicio del juego cada jugador i realiza los pasos siguientes:

1. Genera la información secreta K_i que va a utilizar durante el juego
2. Firma con su clave privada S_i el siguiente mensaje:
   - id_p identificador de la partida
   - $temp$ instante de tiempo en el que se realiza la operación
   - K_i información secreta a utilizar durante el juego.

$$F_i = S_i\{id_p, temp, K_i\}$$

3. Cifra con la clave pública de la TPC (P_{TPC}) el mensaje F_i

$$C_i = P_{TPC}\{F_i\}$$

4. Envía C_i a la TPC.

Una vez la TPC recibe C_i realiza los pasos siguientes:

1. Descifra C_i con su clave privada S_{TPC}, $F_i = S_{TPC}\{C_i\}$
2. Verifica que la firma digital del jugador F_i es válida
3. Comprueba que el identificador de partida id_p corresponde a la partida actual
4. Genera un recibo para el jugador formado por el mensaje firmado

$$R_i = S_{TPC}\{id_p, temp, \mathcal{H}(K_i)\}$$

   donde $\mathcal{H}$ es una función hash unidireccional y libre de colisiones
5. La TPC envía R_i al jugador i
6. Finalmente la TPC almacena de forma segura C_i. La TPC sólo volverá a descifrar C_i si el jugador i abandona

El jugador i verifica los datos y la firma digital de R_i.

Propiedades del protocolo de custodia de claves Mediante la ejecución del protocolo de custodia de claves se garantizan las propiedades siguientes:

Confidencialidad de la información:
El jugador i protege su información secreta y los identificadores de partida con la clave pública de la TPC, P_{TPC}. Sin la clave secreta S_{TPC} se supone que descifrar esta información es intratable.

Integridad de la información: La firma digital F_i garantiza la integridad de los datos que ha enviado el jugador i.

No repudio de la clave: Si un jugador abandona y ha suministrado una información no válida, F_i servirá como prueba de que no ha sido honesto. F_i vincula al jugador i con la información K_i para una partida id_p.

Recibo de juego: El recibo es una prueba de que el jugador ha entregado su clave secreta a la TPC. Al inicio de una partida cada jugador debe mostrar su recibo de juego (junto con $\mathcal{H}(K_i)$). De esta forma el resto tiene la certeza de que la TPC tiene la custodia de su información secreta.

5. Conclusiones y trabajo futuro

En el presente trabajo se ha propuesto un esquema que permite añadir la propiedad de tolerancia al abandono de jugadores a los mejores esquemas de mental poker propuestos en la literatura.

Nuestra propuesta se basa en añadir una Tercera Parte de Confianza al esquema. Esta TPC custodia la información secreta de los jugadores de manera que en caso que alguno de ellos abandone la partida, el resto puede continuar.

La TPC que se añade es secundaria, de manera que solamente interviene en caso de abandono por parte de alguno de los jugadores.

En nuestra investigación futura nos proponemos el objectivo de diseñar un esquema de mental poker con tolerancia al abandono de jugadores sin necesidad de ningún tipo de TPC.

Referencias

1. I. Barany and Z. Furedi, "Mental poker with three or more players", Technical report, Mathematical Institute of the Hungarian Academy of Sciences, 1983.
2. A. Barnett and N. Smart, "Mental Poker Revisited",*Proc. Cryptography and Coding*, Springer-Verlag LNCS 2898, pp 370–383, December, 2003.

3. M. Ben-Or, O. Goldreich, S. Micali and R. Rivest, "A fair Protocol for Signing Contracts", IEEE Transactions on Information Theory, Vol 36, n. 1, pp 40-46, January 1990.
4. En un trabajo previo de alguno de los autores.
5. En un trabajo previo de alguno de los autores.
6. J. S. Chou and Y. S. Yeh, "Mental poker game based on a bit commitment scheme through network", *Computer Networks*, vol. 38, pp. 247-255, 2002.
7. D. Coppersmith, "Cheating at mental poker", in *Advances in Cryptology - Crypto '85* (ed. H. C. Williams), LNCS 218, Berlin: Springer Verlag, pp. 104-107, 1986.
8. C. Crépeau, "A secure poker protocol that minimizes the effect of player coalitions", in *Advances in Cryptology - Crypto '85* (ed. H. C. Williams), LNCS 218, Berlin: Springer Verlag, pp. 73-86, 1986.
9. C. Crépeau, "A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or how to achieve an electronic poker face", in *Advances in Cryptology - Crypto'86* (ed. A. M. Odlyzko), LNCS 263, Berlin: Springer-Verlag, pp. 239-250, 1986.
10. J.L. Ferrer and L. Huguet, "An Efficient Asynchronous Protocol for Optimistic Certified Mail", International Workshop on Cryptographic Techniques and E-commerce, Hong Kong, July 1999.
11. S. Fortune and M. Merritt, "Poker protocols", in *Advances in Cryptology: Proceedings of Crypto'84* (eds. G. R. Blakley and D. Chaum), LNCS 196, Berlin: Springer-Verlag, pp. 454-466, 1985.
12. S. Goldwasser and S. Micali, "Probabilistic encryption & how to play mental poker keeping secret all partial information", in *Proceedings of the 18th ACM Symposium on the Theory of Computing*, pp. 270-299, 1982.
13. C. Hall and B. Schneier, "Remote electronic gambling", in *13th ACM Annual Computer Security Applications Conference*, pp. 227-230, 1997.
14. L. Harn, H. Y. Lin and G. Gong, "Bounded-to-unbounded poker game", *Electronics Letters*, vol. 36, pp. 214-215, 2000.
15. K. Kurosawa, Y. Katayama, W. Ogata and S. Tsujii, "General public key residue cryptosystems and mental poker protocols", in *Advances in Cryptology - EuroCrypt'90* (ed. I. B. Damgaard) LNCS 473, Berlin: Springer-Verlag, pp. 374-388, 1990.
16. K. Kurosawa, Y. Katayama and W. Ogata, "Reshufflable and laziness tolerant mental card game protocol", *TIEICE: IEICE Transactions on Communications/Electronics/Information and Systems*, vol. E00-A, 1997.
17. R. Lipton, "How to cheat at mental poker", in *Proc. AMS Short Course on Cryptography*, 1981.
18. R. Oppliger, "Security Technologies for the World Wide Web", publisher Artech House, Inc, 2002, Computer Security Series, Second Edition.
19. T.P. Pedersen, "A Threshold cryptosystem without a trusted party", *Eurocrypt 91*, LNCS vol 547, pp. 522-526.
20. A. Shamir, R. Rivest and L. Adleman, "Mental poker", *Mathematical Gardner*, pp. 37-43, 1981.
21. C. Schindelhauer, "A toolbox for mental card games", Medizinische Universität Lübeck, 1998. `http://citeseer.nj.nec.com/schindelhauer98toolbox.html`
22. Wai Han Soo, Azman Samsudin and Alwyn Goh, "Efficient Mental Card Shuffling via Optimised Arbitrary-Sized Based Permutation Network", *Information Security*, Springer-Verlag LNCS 2433, pp 446–458, September/October, 2002.

23. M. Yung, "Cryptoprotocols: Subscription to a Public Key, the Secret Blocking and the Multi-Player Mental Poker Game", *Advances in Cryptology Crypto'84*, pp 439-453, 1985, number 196, serie Lecture Notes in Computer Science, 54.
24. W. Zhao, V. Varadharajan and Y. Mu, "Fair on-line gambling", in *16th IEEE Annual Computer Security Applications Conference (ACSAC'00)*, New Orleans, Louisiana, pp. 394-400, 2000.
25. W. Zhao, V. Vadaharajan and Y. Mu, "A Secure Mental Poker Protocol over the Internet", in *Australasian Information Security Workshop*, editor C. Johnson, P. Montague, and C. Steketee, Conferences in Research and Practice in Information Technology, Adelaide, Australia, publisher ACS, vol. 21, pp 105-109, 2003.