Московский Физико-Технический Институт
(Государственный Университет)

Защищенный электронный покер

Студентки 118 группы
Волынец Веры

2005 г.
г. Москва

Введение

С каждым днем популярность сети Интернет растет, появляются огромные возможности получать различные услуги в любое удобное время и в удобном для вас месте. Активно работают Интернет-магазины, осуществляется интерактивная работа клиента с личными счетами в банках, поиск необходимой информации и множество других действий. Для любителей азартных игр существуют так называемые on-line казино, предоставляющие широкий выбор игр и гарантирующие конфиденциальность и безопасность. Преимуществом Интернет-казино, несомненно, является его доступность в течение 24 часов и то, что его услугами можно пользоваться в любой точке земного шара, лишь бы компьютер с выходом в Интернет был под рукой. Самой популярной азартной карточной игрой является покер. Интернет, безусловно, накладывает высокие требования к защищенности и эффективности самого протокола передачи данных во время сеанса игры. В обычном казино каждый игрок видит совершаемые действия соперника, а если даже нет, то все нечестные действия отслеживаются системой видео наблюдения. В электронных казино только надежный протокол может обеспечить соответствующий уровень безопасности.

В основе всех известных и используемых на данный момент протоколов лежат популярные криптографические алгоритмы. Протоколы можно классифицировать на те, в которых участвует доверительное лицо (TTP), и те, в которых данное лицо отсутствует.

1 Протокол, использующий доверительное лицо TTP(trusted third party)

Использование доверительного лица упрощает протокол и уменьшает время его работы. Но существенным недостатком таких протоколов является выбор лица, которому можно полностью доверять, что в итоге оказывается неприемлемым для on-line игр.

Известным протоколом с использованием TTP является протокол, основанный на множественных перестановках. Рассмотрим этапы протокола.

Допустим, в игре участвует 3 человека: Bob, Alice и Charles, а раздатчик карт как доверительное лицо.

1) Раздатчик карт выбирает перестановку π, которая известна только ему.

2) Alice выбирает три перестановки A_a, A_b и A_c.

Аналогично, Bob и Charles выбирают соответствующие три перестановки B_a, B_bи B_c, C_a, C_b и C_c.

Все выше перечисленные перестановки посылаются конфиденциально раздатчику карт. Теперь соответствующий игрок знает свои перестановки, а раздатчик карт знает все.

3) Раздатчик карт вычисляет и передает игрокам следующие значения:

$$\delta_a = B_a^{-1}C_a^{-1}A_a^{-1}\pi^{-1},$$
$$\delta_b = B_b^{-1}C_b^{-1}A_b^{-1}\pi^{-1},$$
$$\delta_c = B_c^{-1}C_c^{-1}A_c^{-1}\pi^{-1}.$$

Если кто-то из игроков захочет вытянуть карту, например Alice, необходимо осуществить следующий протокол:

1) Alice выбирает $y = \pi(x)$ и передает y и $\delta_a(y)$.

2) Bob вычисляет и передает $B_a(\delta_a(y))$.

3) Charles вычисляет и передает $C_a(B_a(\delta_a(y)))$.

4) Затем Alice вычисляет $x = A_a(C_a(B_a(\delta_a(y))))$.

5) В итоге все игроки знают, что набор карт y = π(x) на руках у Alice.

Данный протокол гарантирует, что карты, которые получает игрок, находятся только у него, и только он знает, что это за карты. Очевидно, что если хотя бы один из игроков и раздатчик карт играют честно, то даже остальные, подговорившись, не смогут получить информацию о чужих картах. Проблема этого протокола, помимо наличия доверительной стороны, заключается еще и в том, что жульничество может быть раскрыто только по окончании игры, а не во время действия протокола.

2 Протоколы без доверительного лица

2.1 Протокол на основе криптосистемы Шамира, Риверста, Аделмана

Этот протокол основан на коммутативном свойстве криптофункций [1].
Пусть E_a и D_a функции шифрования и дешифрования Alice, соответственно, E_b и D_b Boba. Alice и Bob договариваются о большом простом числе p и выбирают каждый для себя секретный ключи k=A и k=B соответственно. Причем так, что gcd(A,p-1)=gcd(B,p-1)=1, $E_k \equiv x^k \pmod p$ и $D_k \equiv x^z \pmod p$, где $kz \pmod{p-1} \equiv 1$. Вышеупомянутая система обладает коммутативным свойством, то есть $E_A(D_B(x)) = D_B(E_A(x))$, $E_B(D_A(x)) = D_A(E_B(x))$, $E_A(E_B(x)) = E_B(E_A(x))$, $D_A(D_B(x)) = D_B(D_A(x))$.
В таком случае игра между Bob и Alice будет проходить в следующем порядке:

1) Alice шифрует своей функцией шифрования E_A каждую из 52 карт колоды по отдельности. Затем посылает набор $\{E_A(1),\ldots,E_A(52)\}$ в произвольной последовательности Boby.
2) Bob выбирает пять зашифрованных карт, например $\{ E_A(3), E_A(10), E_A(21), E_A(33), E_A(51)\}$ и отсылает их Alice. Теперь у Alice на руках карты{3,10,21,33,51}.
3) Bob выбирает из оставшихся в колоде еще пять карт и посылает их в зашифрованном виде Alice $\{E_B(E_A(5)), E_B(E_A(8)), E_B(E_A(19)), E_B(E_A(36)), E_B(E_A(49))\}$.
4) Alice дешифрует их и посылает их Boby $\{E_B(5), E_B(8), E_B(19), E_B(36), E_B(49)\}$. Теперь Bob может получить свой набор{5,8,19,36,49}.
5) В конце игры они могут обменяться ключами и проверить друг друга на честность.

У такой системы шифрования есть несколько серьезных недостатков.
Во-первых, игра ограничивается только двумя участниками. Во-вторых, протокол не безопасен с точки зрения утечки информации о картах, находящихся на руках у игроков. В 1981 году Липтон заметил, что по крайне мере один бит информации о карте может стать известен. Для числа x, если $x \equiv y^2 \pmod n$ для некоторого y, то x - квадратичный остаток по модулю числа n. Если все ключи k нечетные числа, то $x^k \pmod n$, где n=p-1, является квадратичным остатком, тогда и только тогда, когда x является квадратичным остатком. Следовательно, если игроки знают, какие карты являются квадратичным остатком и сравнят их с зашифрованными картами, то уже бит информации о каждой карте известен.

2.2 Протокол на основе шифра Эль-Гамаля

В игре, которая проводится по протоколу, основанному на шифре Эль-Гамаля, может участвовать несколько игроков. Но для наглядности ограничимся только двумя: Alice и Bob. Оба участника используют одно и то же простое число p. У каждого из них имеется

$K_A=\{(p,\alpha_A,k_A,\beta_A): \beta_A = \alpha_A^{kA} \pmod p\}$

$K_B=\{(p,\alpha_B,k_B,\beta_B): \beta_B = \alpha_B^{kB} \pmod p\}$

Рассмотрим, как производится шифрование и дешифрование в системе Эль-Гамаля.
Шифрование:
Пусть x сообщение, которое нужно передать.
Alice выбирает произвольное число r_A и шифрует сообщение с помощью K_A:

$y_{1A}= \alpha_A^{rA} \bmod p$
$y_{2A}= x\ \beta_A^{rA} \bmod p$

Затем Bob выбирает произвольное число r_B и продолжает шифрование с помощью K_B:

$y_{1B}= \alpha_B^{rB} \bmod p$
$y_{2AB}= x\beta_A^{rA}\beta_B^{rB} \bmod p$

Дешифрование
Пусть Alice дешифрирует в первую очередь:

$dK_A(y_{1A,}\ y_{2AB})= y_{2AB}(y_{1A}^{kA})^{-1}= y_{2B} \bmod p.$

Теперь Bob применяет свой ключ:

$dK_B(y_{2B})= y_{2B}(y_{1B}^{kB})^{-1}= x \bmod p.$

Очередность выполнения шифрования и дешифрования игроками не играет роли, так как $y_{2AB}= y_{2BA}$.
Опишем теперь сам протокол, необходимо подчеркнуть, что в нем используется цифровая подпись, что существенно улучшает его защищенность от атак и от нечестных действий самих игроков.
Исходные данные
1) Alice и Bob одно и тоже представление 52 карт {1,2…,52}.

2) Alice и Bob договариваются об одном и том же большом простом числе.

3) Alice выбирает пару ключей:

$$K_A=\{(p,\alpha_A,k_A,\beta_A): \beta_A = \alpha_A^{kA}(\bmod p)\}$$

Alice имеет открытый и закрытый ключи: ska-для подписи.

4) Bob, соответственно, имеет:

$$K_B=\{(p,\alpha_B,k_B,\beta_B): \beta_B = \alpha_B^{kB}(\bmod p)\}$$

pkb,skb.

Перемешивание карт

1) Alice выбирает секретное произвольное число r_A и шифрует каждую карту:{$E_A(1)$, $E_A(2)$,…,$E_A(52)$} в произвольном порядке. Затем находит хэш-функцию от r_A, подписывает её $<H(r_A)>_{ska}$ и посылает Boby набор зашифрованных карт и подписанную хэш-функцию.

2) Bob проделывает аналогичные действия с исходным набором и получает :{$E_B(1)$, $E_B(2)$,…,$E_B(52)$} и $<H(r_B)>_{skb}$ и посылает результат Alice.

3) Теперь Alice шифрует карты, полученные от Boba, и вычисляет{$E_{BA}(1)$,

$E_{BA}(2),\ldots,E_{BA}(52)\}$.

4) Аналогично Bob шифрует набор карт, полученных от Alice, и получает $\{E_{AB}(1), E_{AB}(2),\ldots,E_{AB}(52)\}$.

5) Alice сравнивает два набора карт $\{E_{BA}(1), E_{BA}(2),\ldots,E_{BA}(52)\}$ и $\{E_{AB}(1), E_{AB}(2),\ldots,E_{AB}(52)\}$. Если они не совпадают, то протокол был нарушен и его действие будет остановлено. Иначе Alice подписывает карты. Определим $C[n]=E_{AB}(n)$, n=1,…,52. Alice. вычисляет $\{<H(C[1])>_{ska},\ldots,<H(C[52])>_{ska}\}$, подписывает порядок карт $<C[1],\ldots,C[52]>_{ska}$ и посылает Boby два полученных набора.

6) Bob проверяет набор дважды зашифрованных карт и подпись Alice.
Аналогично Alice Bob сравнивает два набора карт, зашифрованных в разном порядке. Если они совпадают, то Bob подписывает карты и их порядок, в итоге получаем: $\{<H(C[1])>_{ska,skb},\ldots,<H(C[52])>_{ska,skb}\}$ и $<C[1],\ldots,C[52]>_{ska,skb}$.

Теперь колода карт готова для проведения честной игры.

Раздача карт

Колода состоит из 52 карт, зашифрованных и подписанных одновременно Alice и Bob. Пусть каждой карте в колоде соответствует порядковый номер:{1,…,52}. Карты, полученные игроками на руки во время игры, должны быть удалены из колоды. Получение из колоды карты игроком осуществляется по следующему протоколу:
1) Пусть Alice хочет вытянуть карту m, где m-порядковый номер от 1 до 52.
Она посылает m и $<H(m)_{ska}>$ Boby.

2) Bob проверяет подпись Alice, дешифрует дважды зашифрованную карту m. Первоначальный порядок карты n, следовательно, карта m является C[n]. После того как Bob дешифрует ее, Alice посылается $E_A(n)$ и $<m,H(E_A(n))>$. Карта m удаляется из колоды Boba.

3) Alice проверяет подпись Boba и получает карту, дешифруя $E_A(n)$. Карта m удаляется из ее колоды.

По окончанию игры участники обмениваются секретными произвольными числами r_A и r_B, чтобы проверить, не имел ли место обман.

Анализ безопасности

Как говорилось ранее, алгоритм, предложенный Шамиром. Риверстом, Аделманом, не подходит для честной и безопасной игры, так как хотя бы один бит о карте может быть известен. Другим его недостатком является ограничение на количество участников. Протоколы с участием третьей доверительной стороны неприемлемы принципиально, так как именно выбор этого лица является большой трудностью, ведь нельзя не учитывать человеческий фактор.
Протокол, основанный на алгоритме Эль-Гамаля, удовлетворяет требованиям к защищенности:
1) Нет доверительного лица.
2)Полное скрытие карт во время игры.
3)Любое количество участников.
4)Защищенность от сговора между игроками. Даже если два игрока договорятся, они не смогут узнать карты третьего игрока, так как карта шифруется каждым участником.

5)Конфиденциальность стратегии игроков.
Во многих протоколах в конце игры приходится раскрывать все карты, следовательно, все будут знать, блефовал ли игрок или нет. Но игроки никогда не желают раскрывать свою стратегию. Поэтому протокол можно немного изменить, добавив дилера, который будет знать только числа <H(r)> и действия игроков, но не будет знать их карты. В конце дилер проверит честность игры, а стратегии соперников останутся в тайне.
6) Отсутствие объемных вычислений.

Недавно была предложена атака на протокол, основанный на шифре Эль-Гамаля [4].
В [4] утверждается, что без большого объема вычислений все-таки можно узнать наименование карты. Пусть x_i- наименование карты, которое известно всем игрокам.
В момент, когда игроки тянут карты из колоды, ее наименование скрыто под неким множителем $f_h= \beta_A^{rA}\beta_B^{rB}$, зная который можно знать значение всех карт, не зная секретные ключи r_A и r_B.
Предложенная атака:
1) Пусть x_{i1},x_{i2} ($i_1 \neq i_2$) две карты как исходные карты.
2) Нечестный игрок вычисляет x_{i1}^{-1} и x_{i2}^{-1} по модулю p.
3) Когда игрок умножает каждую дважды зашифрованную карту y^i_{2AB} на x_{i1}^{-1}, он получает первое множество D_1. Проделав аналогичные действия с картой x_{i2}^{-1}, получим множество D_2.
4) Найдется некоторое значение $f_h= D_1 \cap D_2$.
5) При известном f_h, легко находится $f_h^{-1} \bmod p$.

И все-таки существует протокол, на который еще не была предложена атака.
Протокол, основанный на гомоморфичном шифровании
Протокол описан в статье [5], достаточно сложный протокол, с большим количеством действий и вычислений.
Но он полностью защищен от различных атак и потерь данных при игре.

Список литературы
Все статьи можно найти на сайте www.portal.com или http://citeseer.ist.psu.edu.
[1] Shamir, A, Rivest, R. & Adleman, L. 1979, Mental Poker, MIT/LCS/TM125, Laboratory for Computer Science, Massachusetts Institute of Technology, 545 Technology Square, Cambridge, MA 02139 (www.portal.com).

[2] W. Zhao, V. Vadaharajan and Y. Mu, "A secure mental poker protocol over the Internet", in *Proc.Australasian Information Security Workshop*, Adelaide, Australia. Conferences in Research and Practice in Information Technology, Australian Computer Society.

[3] Рябко Б. Я., Фионов А. Н. «Основы современной криптографии» изд. Научный мир, 2004г, стр. 61-64.
[4] J. Castella-Roca, J. Domingo-Ferrer, 2004, On the Security of an Efficient TTP-Free Mental Poker Protocol, International Conference on Information Technology: Coding and Computing (ITCC'04).
[5] J. Castella -Roca, J. Domingo-Ferrer, 2003, "Practical Mental Poker without TTP based on homomorthic encryption" in *Progress in Cryptologe'2003*.