Безопасный Мысленный Протокол Игры в Покер По Интернету.

Введение.

Сегодня существует достаточное количество устойчивых криптографических алгоритмов и основной задачей является создание безопасных и эффективных криптографических протоколов для предотвращения или обнаружения вредительства и мошенничества. Опишем для начала ,в общем работу криптографии и криптографического протокола. Криптография решает различные проблемы ,такие как проблемы секретности ,проверки подлинности, целостности и человеческой нечестности .Порядок действий, предпринимаемый двумя или более сторонами, предназначенный для решения определенной задачи называется протоколом .Протокол выполняется в определенной последовательности, с начала до конца .Каждое действие должно выполняться в свою очередь и только после окончания предыдущего .Для реализации протокола требуется по крайней мере два человека .Протокол должен приводить к какому-то результату. Каждый участник протокола должен знать протокол и последовательность составляющих его действий. Каждый участник протокола должен согласиться следовать протоколу. Каждое действие должно быть определено так, чтобы не было возможности непонимания. Каждой возможной ситуации должно соответствовать определенное действие. Выполнение протокола происходит по действиям, линейно, пока не будет команды перейти к следующему действию. Каждое действие включает, по крайней мере, одно из двух: вычисления, выполняемые одной или несколькими сторонами, или сообщения, которыми обмениваются стороны. Если мы используем криптографию в протоколе, то это криптографический протокол. Предназначение протокола выходит за рамки простой безопасности, а сам криптографический протокол включает в себя некоторый криптографический алгоритм.

В этом документе рассматривается протокол мысленного покера, который позволяет играть в покер без возврата карты в колоду .В 1979 Шамир, Райвест и Эдлеман предложили схему игры в “Мысленный Покер ”. После этого, было сделано много попыток для достижения протокола, который позволил бы людям играть в “ Мысленный Покер ” (Форчун и Меррит 1985,Шамир,Райвест и Эдлеман 1981,Голдвассер и Микали 1982, Юнг 1985, Крепио 1994).

С ростом и популяризацией Интернета , азартные игры в режиме реального времени становится все более и более важными. Мысленный покер - одна из наиболее популярных азартных игр режима он-лайн. Для целей интерактивной, азартной игры нужно рассмотреть дополнительные требования для протокола покера. Необходимость в безопасных и эффективных протоколах для игр в карты становятся все более и более существенной.

Было несколько протоколов, основанных на криптографии с открытым ключом, описанных в литературе для игры в Мысленный покер (Шамир 1981,Липтон 1981,Голдвассер 1982,Юнг 1985,Форчун 1985, Копперсмит 1986,Куросава и Огата 1991). Эти протоколы требуют ,чтобы игроки генерировали новые пары ключей для каждой игры, которую они играют, что может вызывать интенсивные вычисления. Многие из протоколов небезопасны в выполнении, и они пропускают часть информации относительно самих карт. Несколько протоколов основано на множественных перестановках, которые требуют введения в игру доверенного Продавца Карт. (Холл 1997,Форчун 1985). Если игры в карты используются для целей интерактивной, азартной игры, предположение о полностью доверенном Продавце Карт не приемлемо. Несколько протоколов (Крепио 1986,1994) не имеют никакой информационной утечки, и выполняют многие из важных требований реальной игры в покер, но они не практичны в выполнении. Протоколы используют доказательство с нулевым знанием, и они неэффективны в перетасовке и раздаче карт. Нас интересует эффективный и защищённый мысленный протокол покера, который может удовлетворять всем главным потребностям настоящего протокола покера. В этом документе описан протокол покера, основанный на множественном шифрование и расшифрование индивидуальных карт .Протокол обеспечивает конфиденциальность карт и эффективность в реальном выполнении. Протокол подходит для любого числа игроков для игры в карты по Интернету. Эффект сговора минимален и стратегии игроков конфиденциальны с введением Дилера.

Раздел 1 обсуждает обычные протоколы мысленного покера. Индивидуальная криптографическая система карт и криптографическая система перестановки описана в этом разделе.

Раздел 2 описывает систему множественного шифрования и расшифрования, которая будет основным компонентом нашего мысленного протокола покера.

Раздел 3 описывает подробности нашего мысленного протокола покера. В этом разделе определена инициализация карт, перетасовка набора карт и раздача карт.

Раздел 4 обсуждает защитные свойства нашего протокола.

Раздел 5 предоставляет выводы.

1. Обычные протоколы Мысленного Покера.

1.1 Протокол, основанный на Индивидуальной Криптографической системе Карт.

Шамир , Райвест и Эдлеман использовали коммутативные криптографические системы для развития своего мысленного протокола покера. Пусть E_A и D_A будут функциями шифрования и расшифрования Алисы, E_B и D_B, будут функциями шифрования и расшифрования Боба соответственно. В реальном выполнении, Алиса и Боб договариваются о большом простом числе p, и соответственно выбирают секретные ключи k = A и k = B, где gcd(A, p-1) = gcd(B, p-1) = 1. Тогда $E_k(x) \equiv x^k \pmod p$ и $D_k(x) \equiv x^z \pmod p$,где $kz \equiv 1 \pmod{p-1}$. Вышеупомянутая криптографическая система является коммутативной криптографической системой. Для всех сообщений x,
$E_A(D_B(x)) = D_B(E_A(x)), E_B(D_A(x)) = D_A(E_B(x)), E_A(E_B(x)) = E_B(E_A(x)), D_A(D_B(x)) = D_B(D_A(x))$
, Алиса и Боб будут играть игру следующим образом:

1.В криптографической системе используется колода карт {1, ..., 52} .Алиса шифрует каждую карту в колоде отдельно. Алиса посылает набор { E_A (1), ..., E_A (52)} в произвольном порядке к Бобу.

2. Боб выбирает пять зашифрованных карт наугад. Например { E_A (6), E_A (8), E_A (17), E_A(25), E_A(33)} и посылает их Алисе. Алиса может знать, что это карты - {6, 8, 17, 25, 33}.

3.Боб выбирает пять различных зашифрованных карт, для , например { E_A (3), E_A (11), E_A (19), E_A (23), E_A (41)}, зашифрует их, и посылает их назад Алисе, как беспорядочно выбранный набор { E_B (E_A (3)), E_B (E_A (11)), E_B (E_A (19)), E_B(E_A (23)), E_B (E_A (41))}.

4.Алиса расшифровывает карты одну за другой и пересылает
Бобу итоговый набор { E_B (3), E_B (11), E_B (19), E_B (23), E_B (41)}. Боб может расшифровать и получить {3,11, 19, 23, 41}.

5. В конце игры, они могут обменивать свои
шифровальные ключи и проверять, что все игроки играли честно.

Липтон(Липтон1981) наблюдал, что вышеупомянутое выполнение даёт утечку по крайней мере одного бита информации. Для номера x, если $x \equiv y^2 \pmod n$ для некоторого y, x модуль квадратичного вычета n; иначе, x не квадратичный остаток. Все ключи должны быть нечетные числа и $x^k \pmod n$ - квадратичный вычет ,если и только если x есть. Если игроки знают, какие карты являются квадратичными остатками и сравнивают их с зашифрованными картами, игроки могут получить один бит информации на карту. Липтон обеспечил некоторые предложения для утечки одного бита информации, но нет никакой гарантии, что этот результат безопасен (Копперсмит 1986).

1.2 Протокол, основанный на криптографической системе перестановки

Ряд протоколов (Холл 1997, Копперсмит 1985,Борани 1983) основан на множественных перестановках. Есть три игрока Алиса, Боб и Чарльз и один Продавец Карт. Они используют следующие шаги для подготовки колоды карт.

1.Продавец Карт выбирает перестановку π.

2. Алиса выбирает три перестановки A_a , A_b ,и A_c .Боб выбирает три перестановки B_a , B_b и B_c . Чарльз выбирает три перестановки, C_a C_b и C_c . Все выше указанные перестановки посланы Продавцу Карт конфиденциально (только отправитель и Продавец Карт знает их).

3. Продавец Карт вычисляет и передает:

$\delta_a = B_a^{-1} C_a^{-1} A_a^{-1} \pi^{-1}$,

$\delta_b = C_b^{-1} A_b^{-1} B_b^{-1} \pi^{-1}$,

$\delta_c = A_c^{-1} B_c^{-1} C_c^{-1} \pi^{-1}$.

Если игрок, например Алиса, хочет вытянуть карту, используется следующий протокол

1.Алиса выбирает $y = \pi(x)$, чего нет в руке у какого-то игрока, и передаёт у и $\delta_a(y)$.

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

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

4. Алиса вычисляет x = A_a (C_a (B_a (δ_a (y)))).

5. Все игроки делают запись, что $y = \pi(x)$ был в руке Алисы.

В конце, все перестановки публикуются, чтобы проверить честность игры. Вышеупомянутый протокол может гарантировать, что игрок может вытягивать карту, которой нет в руке кого-нибудь, и только он может знать, что это за карта. Если Продавец Карт и по крайней мере один игрок честные, тогда нет никакой возможности для игрока или группы игроков, участвующих в сговоре для получения информации о картах, которые не в их собственных руках. Этот протокол требует Продавца карт для выбора случайного π перестановок .Если игра в карты используется для азартной игры, предположение, полностью доверять Продавцу Карт не хорошая идея. Другой аспект этой перестановки основан на схеме покера , что обман может быть обнаружен только в конце игры, а не в течение работы протокола.

2. Многостороннее Шифрование и Расшифрование.

Базируясь на криптографической системе ЭльГамаля, мы обсудим многостороннюю систему шифрования и систему расшифрования. Без потери общности, мы предполагаем, что имеется две стороны A и B. Эти две стороны используют одно и тоже простое число p. Они имеют

$$K_B = \{(p, \alpha_B, k_B, \beta_B) : \beta_B \equiv \alpha B^{k_B} (\mathrm{mod}\ p)\}$$

$$K_A = \{(p, \alpha_A, k_A, \beta_A) : \beta_A \equiv \alpha A^{k_A} (\mathrm{mod}\ p)\}$$

1. Шифрование:

Первоначальное сообщение - x. Выбираем случайный номер r_A, и результат шифрования с K_A имеет две части y_{1A} и y_{2A}:

$$y_{1A} = \alpha_A^{r_A} \bmod p$$

$$y_{2A} = x\beta_A^{r_A} \bmod p$$

B выбирает случайное число r_B и зашифровывает текст шифрования A (фактически B зашифрует y_{2A}) и получаются следующим две части,

$$y_{1B} = \alpha_B^{r_B} \bmod p$$

$$y_{2AB} = x\beta_A^{r_A}\beta_B^{r_B} \bmod p$$

Фактически, не имеется никакого различия A или B шифруется первым; мы получим тот же самый шифротекст y_{1A}, y_{1B}, y_{2AB}.

2. Расшифрование:

Если А использует свой закрытый ключ шифрования для расшифровки первым,

$$d_{K_A}(y_{1A}, y_{2AB}) = y_{2AB}(y_{1A}^{k_A})^{-1} = y_{2B} \bmod p$$

И затем В использует свой закрытый ключ шифрования для расшифровки,

$$d_{K_B}(y_{2B}) = y_{2B}(y_{1B}^{k_B})^{-1} = x \bmod p$$

x - первоначальное сообщение.
Фактически, не имеется никакого различия А или В расшифровывает первым; мы могли бы использовать формулу, чтобы выразить полное , многостороннее расшифрование

$$d_{K_A,K_B}(y_{1A}, y_{1B}, y_{2AB}) = y_{2AB}(y_{1A}^{k_A})^{-1}(y_{1B}^{k_B})^{-1} = x \bmod p$$

Наиболее важная характеристика для вышеупомянутой системы является то, что если различный порядок используется для шифрования, заключительный шифрованный текст - тот же самый. Если различный порядок используется для расшифрования, то может быть получено первоначальное сообщение. В следующем разделе, описан протокол мысленного покера, использующего вышеупомянутые коммутативные криптографические системы.

3. Протокол Мысленного Покера

Предполагаем, что многие игроки играют в честный он-лайновый " Мысленный Покер ". Часть игры в карты включает в себя перетасовку и раздачу карт честным способом. Все игроки должны быть уверенны, что никто не подтасовывал карты. Предполагаем, что нет доверенной третьей стороны, вовлеченной в течение игры. В этом докладе будем фокусировать внимание только на протоколе для перетасовки и раздачи карт. Рассматриваем мысленный протокол покера, который может перетасовывать любую колоду карт. В отличие от протоколов , которые базировались на множественных перестановках (Форчун 1985), этот протокол всегда имеет дело с картами один на один. Без проигрыша в общности, мы предполагаем, что есть два игрока Алиса и Боб. Нет никакого реального различия, в том какое количество игроков должно играть.

3.1 Инициализация

1.Алиса и Боб соглашаются выбирать те же самые 52 карты для 52 карт, которые являются подходящим набором шифрования {1, ..., 52}.

2. Алиса и Боб соглашаются выбирать одинаковое простое число p.

3. Алиса выбирает свои пары ключей для шифрования и расшифрования следующим образом:

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

4. Алиса имеет открытую / закрытую пару ключей pka и ska,ska для подписи и pka для проверки другими.

5. Боб выбирает свои пары ключей шифрования и расшифрования следующим образом:

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

6. Боб имеет пару открытых/закрытых ключей pkb и skb,skb для своей подписи и pkb для проверки другими.

3.2 Перетасовка Карт.

В нашем протоколе, перетасовка карт основана на шифрование индивидуальных карт.

1. Алиса выбирает секретное случайное число r_A, и затем шифрует исходные карты одну за другой.

Набор шифрованных карт - { E_A (1), ..., E_A (52)} в произвольном порядке. Алиса подписывает хеш-функцию из r_A , чтобы получить < $H(r_A)$ >ska. Алиса посылает { E_A (1), ..., E_A (52)} и < $H(r_A)$ >ska к Бобу.

2. Боб выбирает секретное случайное число r_B , и затем шифрует исходные карты одну за другой. Набор шифрованных карт - { E_B (1), ..., E_B (52)} в произвольном порядке. Боб подписывает хеш-функцию из r_B , чтобы получить < $H(r_B)$ >skb. Боб посылает { E_B (1), ..., E_B (52)} и < $H(r_B)$ >skb Алисе.

3. Алиса шифрует набор карт, зашифрованных Бобом , и получает { E_{AB} (1), ..., E_{AB} (52)}. Алиса посылает результаты к Бобу.

4. Боб шифрует набор карт, зашифрованных Алисой , и получает { E_{BA} (1), ..., E_{BA} (52)}. Боб посылает результаты Алисе.

5. Алиса проверяет два набора дважды зашифрованных карт с различным порядком шифрования. Если два набора не равны, тогда протокол будет остановлен. Если они равны, Алиса подписывает дважды зашифрованные карты одну за одной. С системой обозначений $C[n] = E_{AB}(n)$, где (n = {1, ..., 52} – порядковый номер карт), Алиса получает {< $H(C[1])$ >ska,... < H (C [52]) >ska}. Алиса подписывает порядок карт и получает < C [1], ..., C [52] >ska. Алиса посылает дважды зашифрованные карты, подписи карт и подписанный порядок карт к Бобу.

6. Боб проверяет набор дважды зашифрованных карт и подписи Алисы. Боб проверяет два набора дважды зашифрованных карт с различным порядком шифрования. Если проверки успешны, Боб подписывает дважды зашифрованные карты снова и получает { < H (C [1]) >ska,skb, ..., < H (C [52]) >ska,skb}.Боб подписывает порядок карт снова и получает < C [1], ..., C [52] >ska,skb.Боб посылает подписи карт и подписанный порядок карт Алисе.

Теперь колода карт зашифрована Алисой и Бобом их подписями. Основываясь на нашем обсуждении в разделе 2, шифрования в различном порядке дают те же самые результаты. Мы только используем установленный порядок подписи во всех протоколах. Очевидно, если есть большее количество игроков , наш протокол будет работать точно также , как упомянуто выше.

3.3 Раздача карт.

Имеются 52 карты, зашифрованные и Алисой и Бобом. В самом начале, набор доступных порядковых номеров {1, ..., 52}. В течение игры, если некоторые карты в руках игроков, соответствующие порядковые номера удаляются из доступного набора. Когда игрок нуждается в карте, выполняется следующий протокол

1.Алисе нужно вытянуть карту m , m - порядок карты после двойного шифрования. Она посылает m и < H (m) >ska к Бобу.

2.Боб проверяет подпись Алисы и затем проверяет, что m находится в доступном наборе или нет. Если m не в доступном наборе, Боб посылает Алисе соответствующее сообщение. Если m находится в доступном наборе, Боб расшифровывает дважды зашифрованную карту m . Первоначальный порядок карт - n, карта m - это C[n] После расшифрования Бобом m становится $E_A(n)$.Боб посылает $E_A(n)$, < m , H ($E_A(n)$) >skb Алисе. Боб удаляет m из своего доступного набора.

3. Алиса проверяет подпись Боба , и расшифровывает $E_A(n)$ чтобы открыть карту и прибавить к карте в своей руке. Алиса m удаляет из своего доступного набора.

Когда игра закончена, Алиса и Боб показывают свои секретные случайные числа r_A и r_B . И Алиса и Боб могут проверять, обманула ли другая сторона или нет. Стратегия каждого игрока полностью

показана в конце игры. В следующем разделе, мы обсудим, как гарантировать конфиденциальность стратегии.

Если есть много игроков, вышеупомянутые протоколы работают подобным способом. Единственное различие - то, что если игрок нуждается в карте, все другие игроки расшифруют карты одну за другой и обновят свои доступные наборы одновременно. Игрок, который нуждается в карте, может открыть карту и прибавить карту к его / ее руке, и обновить его / ее доступный набор.

4. Обсуждение.

В следующем разделе, обсуждаются важные свойства защиты нашего протокола. Мы также сравниваем наш протокол со старыми протоколами.

(1) Полная Конфиденциальность Карт.

Предыдущие протоколы, основанные на индивидуальных картах имеют недостаток утечку одного бита информации(Липтон 1981, Копперсмит 1986). Липтон обсуждал утечку и дал некоторые предложения для укрепления криптографической системы, например карты, кодируются первоначально так, чтобы они все были квадратичные вычеты (или все не остатки). Но все еще нет никакой гарантии, что результат безопасен. Действительно, показывается, что биты , могут все еще просачиваться. В нашем протоколе, не имеется никакой информации об утечке, потому что шифрование/расшифрование использует стандарт ЭльГамаль криптографической системы.

(2) Без Продавца Карт

Продавец Карт, включён в старые протоколы (Холл 1997,Форчун 1985), которые основаны на множественных перестановках. Честность этого вида протоколов основана на предположение, что Продавцу Карт можно полностью доверять . Для реальной азартной игры, такое предположение – не подходит. Мы не можем принимать существование такой полностью доверенной стороны. Протокол, рассмотренный в этом документе, избавляется от Продавца Карт полностью.

(3) Любое Число Игроков

Удобно расширить протокол большим количеством игроков ,базируясь на коммутативности множественного шифрования и расшифрования,. С одинаковым ,простым числом p, каждый игрок, например X, имеет пару ключей $K_X = \{(p, \alpha_X, k_X, \beta_X) : \beta_X \equiv \alpha X^{k_X} (\mathrm{mod}\ p)\}$

В процессе перетасовки карт, каждый игрок X выбирает секретное случайное число r_X . Все карты много раз зашифрованы всеми игроками. Во время раздачи карт, когда Игрок X вытягивает карту, все другие игроки расшифровывают карту, и только игрок X может открыть карту. Все игроки удаляют карту из доступного набора.

(4) Защита От Сговора Игроков

Протокол может гарантировать минимальный эффект от сговора. Даже если два игрока сговорились, они могут только получить карты друг друга, но не карты третьего игрока. Поскольку каждая карточка много раз зашифрована всеми игроками, карта открыта только в случае, когда все игроки расшифровали карту. Любое подмножество игроков не может знать что-либо относительно карт других игроков. Никакой сговор среди игроков мошенников не может затрагивать карты, вытянутые честным игроком и нетронутые карты.

(5) Полная Конфиденциальность Стратегии

Представленный протокол просит, чтобы игроки показали всю информацию в конце игры. Это делает невозможным блеф для игроков .Настоящие игроки покера никогда не допускают такой игры. К счастью, если включён Дилер, очень просто изменить вышеупомянутый протокол. При перетасовке карт, каждого игрок X выбирает своё секретное случайное число r_X и отсылает < H (r_X) > Дилеру. В течение игры, каждый игрок посылает информацию своего действия (для восстановления в будущем, кроме открытых карт) к Дилеру. В конце игры, каждый

игрок посылает своё секретное случайное число Дилеру. Дилер способен проверить честность целой игры.
В течение игры, информация о картах конфиденциальна для Дилера. Дилер - единственный человек кто может знать стратегию каждого игрока в конце игры. Такое предположение разумно и может быть допустимым. Это намного лучше, чем предположение о Продавце Карт, которому полностью доверяют и он знает всю информацию о картах в течение игры.

(6) Эффективность и Ясность

Криптографическая система, используемая в нашей схеме, основана на криптографической системе ЭльГамаля. Для игры двух игроков, имеются только 104 раза шифрования и расшифрования ЭльГамаля (максимум в одной целой игре). Для игры n игроков, $52 \times n$ шифрований
и $52 \times n$ расшифрования ЭльГамаля (максимум в одной целой игре). Протокол эффективен. Для группы игроков, после установки системы , они могут использовать свои пары ключей шифрования/расшифрования и пары открытых / закрытых ключей для множества игр. Для новой игры, игроки только должны выбрать новые секретные случайные числа (параметры шифрования). Есть несколько других успешных протоколов , основанные на доказательстве с нулевым знанием. К сожалению, они – не практичны и часто очень сложные. Они требуют довольно долгого времени вычисления для перетасовки колоды карт.

5. Заключение.

С ростом популярности Интернет стал важным рынком для он-лайновых азартных игр. Игры в карты широко используются в азартных играх режима он-лайн. Представленная схема протокола мысленного покера достигла главной потребности полной системы покера. Протокол безопасен, эффективен и подходит для любого числа игроков. Протокол избавляется от существования Продавца карт полностью и имеет минимальный эффект от сговора игроков. С введением Дилера, стратегии игроков могут быть сделаны конфиденциальными для других людей (кроме Дилера). В этом случае, Дилер узнаёт стратегии игроков только в конце игры. Однако, игра в которой делается обмен карт имеет некоторые открытые проблемы, которые не решены нашим протоколом, например, как возвращать карту в колоду. Процесс азартной игры требует таких действий как размещение ставок и имеет дело с платежами. Представленный протокол основан на индивидуальных картах. Несложно объединить этот протокол с управляющими протоколами целого процесса азартной игры. Честная схема азартной игры в режиме он-лайн была предложена (Зао , 2000 г.) для гарантии честности интерактивной, азартной игры. Эффективное, справедливое и безопасное решение, основанное на представленной здесь схеме честной он-лайн азартной игры и карточном протоколе , может быть получено.

Литература

Zhao, W. Varadharajan, V. & Mu, Y. 2000, Fair On-line Gambling, 'Proceedings of the 16th Annual Computer Security Applications Conference', ACSAC, pp. 394-400.

Zhao,W. Varadharajan, V & Mu.Y.2000, Secure Mental Poker Protocol Over The Internet, School of Computing and Information Technology University of Western Sydney,NSW 2747, Australia Email: wzhao@cit.uws.edu.au, Department of Computing Macquarie University,NSW 2109, AustraliaEmail: ymu@ics.mq.edu.au , vijay@ics.mq.edu.au .

Брюс Шнайер. Прикладная криптография (перевод на русский язык распространяемый в Интернете).