Архипов Лев Александрович

студент

Кротова Елена Львовна

канд. физ.-мат. наук, доцент

ФГБОУ ВПО «Пермский национальный

исследовательский политехнический университет»

г. Пермь, Пермский край

ПРОТОКОЛЫ ИГРЫ В МЫСЛЕННЫЙ ПОКЕР

***Аннотация**: в данной статье авторами рассматриваются протоколы мысленного покера, которые позволяют играть в покер без возврата карты в колоду.*

***Ключевые слова**: мысленный покер, протокол игр, криптографическая система, карты, ключи, информация.*

Протоколы мысленного покера – это система криптографических задач, касающихся честных игр на расстоянии.

Шамир, Райвест и Эдлеман в 1979 году предложили схему игры в «Мысленный Покер». В современном мире, азартные игры в режиме онлайн стали для многих людей частью их обыденной жизни. Покер – является одной из самых востребованных азартных игр в международной сети. С увеличением востребованности спроса на покер появилась нужда в наиболее защищенных протоколах для игр в карты. Существует несколько протоколов, которые основываются на криптографической системе с открытыми ключами. В данных протоколах должно соблюдаться условие о том, чтобы участники создавали новые пары ключей в каждой игре, что вызывает наиболее сложные задачи. Большинство этих протоколов пропускают сегмент информации о картах игроков. Существуют протоколы, основанные на многочисленных ротациях, требующие ввод в игру доверенного Дилера. Когда речь заходит об азартной игре, то речь о доверие к Дилеру вызывает опасения и сомнения. Небольшое количество протоколов не создают никакой утечки информации, и соответствуют многим важным требованиям реальной игры в покер, но они очень сложны и их трудно воплотить в игре.

Возьмем несколько протоколов и на их примере попробуем разобраться в их изъянах, чтобы в дальнейшем учесть их недочеты и обезопасить людей от обманов или сговоров.

Протокол, основанный на Индивидуальной Криптографической системе Карт

Шамир, Райвест и Эдлеман отдали предпочтение коммутативным криптографическим системам для дальнейшего прогресса своего мысленного протокола покера. Пусть V_a и H_a будут функциями зашифровки и расшифровки Анны, V_b и H_b, будут функциями Бориса соответственно. Анна и Борис согласуют большое простое число p, и после этого выбирают секретные ключи $k = A$ и $k = B$, где НОД $(A, p\text{-}1)$ и НОД $(B, p\text{-}1)$ соответственно равны 1. Тогда $E_k(x) \equiv x^k (\mathrm{mod}\, p)$ и $D_k(x) \equiv x^z \ (\mathrm{mod}\, p)$, где $kz \equiv 1 (mod\ p\text{-}1)$. Данная криптографическая система является коммутативной. Для всех сообщений x:

$$V_a\,(H_b(\mathrm{x})) = H_b(V_a(\mathrm{x})),\ V_b(H_a(\mathrm{x})) = H_a(V_b(\mathrm{x})),\ V_a(V_b(\mathrm{x})) =$$
$$V_b(V_a(\mathrm{x})),\ H_a(H_b(\mathrm{x})) = H_b(H_a(\mathrm{x}))$$

Анна и Борис будут играть следующим образом:

1. В криптографической системе используется колода карт $\{1, \ldots, 52\}$. Анна шифрует каждую карту раздельно. Анна отправляет выборку $\{V_a(1), \ldots, V_a(52)\}$ в хаотичном порядке Борису.

2. Борис из выборки берет пять зашифрованных карт наугад. Например $\{V_a(7), V_a(9), V_a(15), V_a(34), V_a(48)\}$ и отправляет их обратно Анне. Анна может знать, что это карты – $\{7, 9, 15, 34, 48\}$.

3. Борис выбирает пять различных зашифрованных карт, например $\{V_a(4), V_a(12), V_a(20), V_a(29), V_a(51)\}$, шифрует их, и посылает их обратно Анне, как произвольным образом случайный выбранный набор $\{V_b(V_a(4)), V_b(V_a(12)), V_b(V_a(20)), V_b(V_a(29)), V_b(V_a(51))\}$.

4. Анна постепенно расшифровывает карты и в итоге посылает Борису конечный набор выборки $\{V_b(4), V_b(12), V_b(20), V_b(29), V_b(51)\}$. Борис расшифровывает данный набор и получает $\{3,11,19,23,41\}$.

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

При внимательном просмотре можно заметить, что вышеупомянутое решение может совершить случайную утечку одного бита информации. Для номера x, если $x \equiv y^2 (mod\ n)$ для некоторого y, где x должен быть модулем квадратичного вычета n; в противном случае, x не квадратичный остаток. Все ключи должны быть нечетными числами и $x^k (mod\ n)$ – квадратичный вычет, если x есть. Если допустить вариант о том, что игроки знают, какие карты должны являться квадратичными остатками и после этого они сравнивают их с зашифрованными картами, то в данной ситуации игроки могут узнать один бит информации на карту. Можно прийти к выводу, что нет никакой уверенности в том, что результат будет безопасным и честным.

Протокол, основанный на криптографической системе перестановки

Есть три игрока Анна, Борис и Степан и один Дилер. Они используют следующие шаги для подготовки колоды карт:

Дилер выбирает перестановку π.

1. Анна выбирает три перестановки A_a, A_b и A_c. Борис совершает три перестановки B_a, B_b и B_c. Степан также совершает три перестановки C_a , C_b и C_c. Все данные перестановки отправлены Дилеру конфиденциально.

2. Дилер 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 хочет вытянуть карту, используется следующий протокол:

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

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

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

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

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

В итоге, все совершенные перестановки открываются, для того чтобы проверить насколько честной была игра. Вышеупомянутый протокол может обеспечить то, что игроки могут вытянуть карту, которая еще не была использована, и могут быть уверены в том, что только они знают эту карту. Если Дилер и хотя бы один игрок честные, тогда не будет существовать вероятность того, что игрок или группа игроков, которые участвуют в сговоре, получат информацию о картах других игроков. Данный протокол требует наличие Дилера для осуществления случайных π перестановок. В азартной игре всегда есть опасность того, что некоторые игроки или даже сам Дилер состоят в сговоре, этот факт должен быть учтен, поэтому нельзя никогда доверять постороннему человеку, в том числе и Дилеру. Другим аспектом этой перестановки являются то, что он основан на схеме покера, что обман может быть обнаружен только в конце игры, а не в течение работы протокола.

Проанализировав вышеуказанные протоколы, мы можем прийти к выводу, что данные протоколы не достигли главных потребностей покера. Существует вероятность утечки битов, то есть, нет полной конфиденциальности карт. Честность некоторых видов протоколов зависит на предположение, что Продавцу Карт можно полностью доверять. Есть большая вероятность сговора игроков.

Список литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.

2. Zhao W. Proceedings of the 16th Annual Computer Security Applications Conference: Fair On-line Gambling / W. Zhao, V. Varadharajan, Y. Mu // ACSAC. – 2000. – P. 394–400.