Мысленный покер с тремя игроками

Этот протокол решает задачу раздачи карт в открытой сети между игроками без помощи посредника. В данном протоколе рассматривается случай из трёх игроков, но он легко обобщается на большее число участников. Предполагается использование коммутативной криптосистемы с открытым ключом, например, система RSA с общим модулем.

Мысленный покер с тремя игроками

1. Каждый игрок генерирует свою пару ключей (открытый/закрытый), но оба ключа держит в секрете до конца игры.
2. Алиса генерирует 52 сообщения (колоду карт). Например, файлы, имена которых являются номерами от 1 до 52, при этом содержание их должно быть перемешанной колодой при каждой новой генерации колоды. В каждое сообщение необходимо включать уникальную случайную строку с тем, чтобы на последующих этапах протокола Алиса могла проверять их подлинность. Алиса зашифровывает все сообщения с помощью своего открытого ключа и отсылает их Бобу.
3. Боб не может прочитать колоду. Но чтобы и Алиса по именам файлов не могла отследить карты, он перемешивает имена файлов. С этого момента перемешивание колоды окончено, и имена файлов не перемешиваются до конца игры. Теперь Боб произвольно отбирает пять из них, шифрует их своим открытым ключом и отправляет Алисе.
4. Боб отсылает остальные 47 сообщений Кэрол.
5. Кэрол, которая не может прочесть ни одного сообщения, произвольно отбирает пять из них, шифрует их своим открытым ключом и отправляет Алисе.
6. Алиса, которая не может прочесть ни одного из полученных сообщений, расшифровывает их своим закрытым ключом и отсылает обратно Бобу или Кэрол, в зависимости от того, от кого она их получила.
7. Боб и Кэрол расшифровывают сообщения с помощью своих ключей, чтобы узнать, какие карты им достались.
8. Кэрол произвольно отбирает пять из 42 оставшихся сообщений и отправляет их Алисе.
9. Алиса расшифровывает сообщения, чтобы узнать свои карты.
10. Колода осталась у Кэрол. Если кому-то (кроме Алисы) нужно добрать карты, то Кэрол отправляет ему оставшуюся колоду, и он повторяет протокол в Алисой. Если карты нужны Алисе, то тот, у кого в данный момент находится шифрованная колода, отсылает ей произвольно выбранные карты в количестве запроса.
11. По окончании игры Алиса, Боб и Кэрол открывают свои карты и пары ключей с тем, чтобы каждый мог убедиться в отсутствии мошенничества.

Однонаправленный сумматор

Постановка задачи состоит в следующем. Алиса является членом тайной организации. Надо найти способ, чтобы Алиса всякий раз могла точно опознать члена организации, желательно не видя или не зная его имени и лица.

Возможны несколько решений. Например, каждый член может иметь список всех членом организации. Но тогда одна компрометация выдаёт всю организацию. Другой способ — это пароль. Но пароль легко может перейти третьим лицам без всякой подделки даже случайным образом. Следующий уже более надёжный способ — это членский билет или какая-либо идентификационная карточка, подготовленная доверенным секретарем. Здесь есть возможность подделки, или кражи. Наконец, самым слабым звеном может оказаться доверенный секретарь. Следующий способ не требует таких материальных вложений и в то же время хорошо решает поставленную задачу — это однонаправленный сумматор.

Однонаправленный сумматор

Однонаправленный сумматор — это нечто вроде однонаправленной хэш-функций, только коммутативной. Она позволяет хэшировать базы данных членов организации в любом порядке, но всегда получать одно и то же значение. Более того, в хэш можно добавлять новых членов и получать новый хэш, опять же не зависящий от порядка.

Тогда протокол аутентификации по принадлежности некоторой организации выглядит следующим образом. Алиса выполняет вычисления, используя множество всех имен членов союза, кроме своего собственного, получает значение Σ_A. Затем Алиса сохраняет полученное значение вместе со своим именем, т.е. пару $\{\Sigma_A, A\}$. То же самое делает Боб, его пара $\{\Sigma_B, B\}$, и остальные члены союза.

Теперь, когда они встречаются, они обмениваются своими парами и проверяют равенство $\Sigma_A + A = \Sigma_B + B$. Если равенство выполняется, то они оба состоят в этом тайном союзе.

Существует простая функция однонаправленного сумматора.

Генерируется число n как произведение двух простых чисел, и x_0 случайное ($1 < x_0 < n$) взаимно простое с n. Тогда функция определяется выражением $A(x_i, y) = x_{i-1}{}^{y} \bmod n$. Если $y_1, y_2, y_3, \ldots, y_k$ — это имена членов организации, то

$$\Sigma_i = (\ldots((x_0^{y_1} \bmod n)^{y_2} \bmod n)^{y_3} \ldots)^{y_k} \bmod n,$$

где отсутствует степень y_i, откуда получаем пару $\{\Sigma_i, y_i,\}$. Тогда для любых i, j ($i \neq j$, $1 \leq i, j \leq k$) выполняется равенство $\Sigma_i{}^{y_i} \bmod n = \Sigma_j{}^{y_j} \bmod n$. Раздачу пар может осуществлять центр, а может создавать и каждый член, если имеет значения n, x_0, y_1, y_2, y_3, …, y_k. Чтобы включить в список новых членов, достаточно просто послать по кругу новые имена. К сожалению, удалить члена можно только одним методом: разослать всем членам новый список. Однако делать это придется только при отставке кого-то из членов; умершие члены могут оставаться в списке. (Действительно, странно — почему это мертвецы никогда не создают проблем?)

Раскрытие секретов «всё или ничего»

Допустим, Алиса торгует секретами. Разумеется, Алиса не желает отдавать два секрета по цене одного и не показывает даже малейшей части информации, касающейся любого секрета. Однако и Боб, потенциальный покупатель, не желает покупать кота в мешке. Кроме того, он не хочет сообщать Алисе, какие секреты ему нужны. В этом случае протокол покера не сработает, поскольку по завершению этого протокола Алиса и Боб должны раскрыть друг другу свои карты.

Решение проблемы называется *раскрытием секретов «все или ничего»* (All-Or-Nothing Disclosure Of Secrets — ANDOS). Суть его заключается в том, что если Боб получил любую информацию о любом секрете Алисы, он теряет шанс узнать что-либо еще о других её секретах. Если есть уверенность, что участники этого рынка не могут создавать коалиции (т.е. достаточно честны), то можно использовать следующий простой протокол.

1. $A \rightarrow B$:$\{C_i\}$, где $C_i = S_i^e \bmod n$, т.е. Алиса зашифровывает все секреты с помощью RSA и посылает их Бобу;
2. $B \rightarrow A$: $\{C'\}$, где $C' = C_b \cdot r^e \bmod n$, т.е. Боб выбирает свой секрет C_b, генерирует случайное число r и посылает Алисе $C' = C_b \cdot r^e \bmod n$;
3. $A \rightarrow B$:$\{P'\}$, где $P' = C'^{\,d} \bmod n$ $(= S_b\, r)$;
4. B: Боб вычисляет $S_b = P'\, r^{-1} \bmod n$

Если участники могут создавать коалиции, т.е. жульничать, Боб перед проходом 2 может доказать с нулевым разглашением, что он знает некоторое r, такое что $C' = C_b\, r^e \bmod n$, и хранить b в секрете, пока Алиса не передаст ему на проходе 3 значение P'.