Византийское соглашение и покер по телефону

Ю. Лифшиц*

30 сентября 2005 г.

План лекции

1. Неформальная постановка задач
2. Византийское соглашение
3. Покер по телефону
4. Пример работы византийского протокола

1 Неформальная постановка задач

1.1 Автопилоты

Представим себе, что по небу летит самолет. На автопилоте. А теперь представим, что этот автопилот сломался. Ничего хорошего не произойдет, не так ли? Как бороться с такой ситуацией? Ясное дело, поставить еще один независимый автопилот. Но которого из них слушаться, когда они дают разные указания? Из двух автопилотов ни один не способен образовать большинство. Значит, надо поставить три автопилота! Даже если один из них сломается, остальных все равно будет больше, и они смогут принять правильное решение голосованием! Но кто будет проводить это голосование? Некий контрольный центр? Но если сломается он, то все усилия пойдут насмарку. Значит, автопилоты должны договориться между собой и сами прийти к правильному решению.

К сожалению, это невозможно. Вернее, это невозможно для трех автопилотов. А вот для четырех, из которых испортилось не более одного, необходимый протокол существует, и он будет предъявлен.

*Законспектировал А. Девский.

1.2 Карты по телефону

Предположим, что неугомонные Алиса и Боб решили сыграть в карты. Вот только они живут в разных городах, и из средств связи у них есть только телефон. Казалось бы, сыграть честную партию по телефону невозможно. И это действительно невозможно. Но, с другой стороны, протокол для такой игры известен довольно давно, и он будет предъявлен. Почему в этих двух утверждениях нет противоречия? Попробуйте догадаться сами, а если не догадаетесь - в конце третьего раздела мы вам расскажем.

2 Византийское соглашение

2.1 Византийские генералы

В изначальной постановке задачи никаких автопилотов не было, а было n византийских отрядов, осаждающих вражеский город. Каждым отрядом командовал независимый генерал. Генералы могли общаться друг с другом по закрытому каналу, например, с помощью голубиной почты. Все вместе они общаться не могли, потому что отряды стояли далеко друг от друга, а радио и Интернет еще не изобрели. Все знали, что враг хитер и коварен, и вполне мог подкупить кого-нибудь из генералов; оставалось надеяться, что генералов-предателей не очень много. Тем временем осада затягивалась, пора было переходить к решительным действиям. Да вот беда - генералы не могли собраться вместе и выработать единый план. Если бы не угроза предательства, все было бы просто - каждый генерал изложил бы остальным свой план с помощью голубей, а затем каждый выбрал бы наиболее популярный план и действовал бы согласно ему. Но так поступить нельзя - а ну как предатель скажет одному генералу, что пора наступать, а другому - что лучше отойти? Половина генералов рванется в бой, половина отступит, и получится черт знает что.

Таким образом, нужен был протокол, отвечающий двум требованиям:

1. Все честные генералы должны в итоге принять одно и то же решение.
2. Если предателей не очень много, то это решение должно оказаться правильным.

Сам протокол, по-видимому, должен состоять из двух фаз:

Фаза 1. Генералы обмениваются информацией.

Фаза 2. Генералы принимают решение на основе полученной информации.

Если мы в ходе первой фазы сделаем так, чтобы все генералы получили одинаковую сводку информации, то вторая фаза будет очень простой - выбрать наиболее популярный план из n предложенных. Таким образом, от первой фазы мы требуем два условия:

1А. Информация честных генералов должна дойти до остальных неискаженной.

1Б. От любого генерала все должны получить одинаковую информацию, даже если он попытается сообщить разную.

Далее мы для простоты будем считать, что каждый генерал делает бинарный выбор, например, выбирает между атакой и отступлением.

2.2 Командир и его заместители

Ясно, что изложенная выше задача разбивается на n одинаковых подзадач - каждый генерал должен передать свой выбор остальным. Эти подзадачи эквивалентны задаче о командире, который должен передать свой приказ $n-1$ заместителям, причем предателями могут быть как заместители, так и командир. От такого протокола мы опять потребуем два похожих свойства:

1. **Согласованность** Все честные заместители должны поступить одинаково.

2. **Исполнительность** Если вдобавок командир честен, то есть отдал всем одинаковый приказ, а среди заместителей не слишком много предателей, то все честные заместители должны поступить так, как приказал командир.

В этой схеме каждый может общаться с каждым. Докажем от противного, что для $n = 3$ и не более чем одного предателя требуемый протокол невозможен.

Первая ситуация. Пусть командир и первый заместитель - честны, а второй заместитель - предатель. Командир отдает приказ атаковать, однако второй заместитель, желая запутать первого, говорит ему, что командир приказал отступать. Наш предполагаемый протокол должен обладать исполнительностью, поэтому честный первый заместитель должен выполнить приказ командира, то есть пойти в атаку, игнорируя своего коллегу. Таким образом, выходит, что заместитель должен в любом случае слушаться командира.

Вторая ситуация. Пусть теперь предатель - командир. Он отдает первому заместителю приказ атаковать, а второму - отступать. Честные заместители честно сообщают друг другу эти приказы, но, согласно предыдущему выводу, игнорируют разночтения, так что первый заместитель идет в атаку, а второй отступает. Стоп! Мы потеряли согласованность.

Это и доказывает невозможность такого протокола.

2.3 Протокол для $n \geq 3m + 1$

В предыдущем пункте беда была в том, что предателей было *не менее одной трети*. Сейчас мы построим протокол, обладающий нужными свойствами, если предателей менее одной трети. Строить будем по индукции по числу

m, где, как потом окажется, m - это максимальное число предателей, для которого протокол все еще работает. Напомним, что мы сейчас рассматриваем не задачу о генералах, а более простую задачу о командире и заместителях, причем с бинарным выбором приказа.

Протокол $BG(0)$.

1. Командир рассылает заместителям приказ.
2. Заместители поступают в соответствии с полученным от командира приказом.

Заметим вскользь, что для случая, когда предателей нет, протокол прекрасно работает.

Протокол $BG(m)$.

1. Командир рассылает заместителям приказ.
2. Каждый заместитель рассылает этот приказ своим коллегам, используя протокол $BG(m-1)$. На время рассылки рассылающий заместитель играет роль «командира» среди своих коллег.
3. Каждый заместитель из $n-1$ приказа (одного «своего» и $n-2$ полученных от коллег) выбирает наиболее часто встречающийся и поступает в соответствии с ним.

Тут необходимо сделать одну оговорку. К сожалению, может случиться так, что наиболее частого плана не будет (рассмотрите самостоятельно случай, когда командир-предатель приказывает одной паре честных заместителей атаковать, а другой - отступать, используя протокол $BG(1)$). Поэтому мы будем считать, что заранее оговорен «план по умолчанию», которому все следуют в случае «ничьей».

Лемма. Для любых натуральных чисел k, m протокол $BG(m)$ обладает исполнительностью, если $n \geq 2k + m + 1$, а предателей не больше k.

Доказательство. Индукция по m.

База: $m = 0$**.** В самом деле, все честные заместители поступят в соответствии с полученным правильным приказом.

Переход: $m - 1 \mapsto m$**.** Всякий честный заместитель, получив приказ, рассылает его коллегам по $BG(m-1)$. При этом участников этой рассылки $n - 1$ (все, кроме командира), то есть не менее $2k + m$, а предателей среди них по прежнему не более k. По предположению индукции, в этом случае $BG(m-1)$ обладает исполнительностью, а стало быть, честные заместители правильно передадут коллегам правильный приказ командира. В этом случае у каждого заместителя окажется не менее $k + m + 1$ правильных копий приказа (не более чем k предательских копий окажутся неправильными), а это в любом случае больше половины. Таким образом, каждый честный заместитель выполнит правильный приказ.

Доказательство завершено.

Теперь докажем основную теорему.

Теорема о корректности $BG(m)$**.** Для любого натурального m протокол $BG(m)$ обладает согласованностью и исполнительностью, если $n \geq 3m + 1$, а предателей не более m.

Доказательство. Исполнительность следует из леммы при $k = m$. Согласованность будем доказывать по индукции по m.

База: $m = 0$**.** Раз предателей нет вовсе, то все получат одинаковый приказ и выполнят его.

Переход: $m-1 \mapsto m$**.** Если командир честен, то согласованность следует из исполнительности (все правильные приказы одинаковы), а исполнительность уже доказана. Пусть теперь командир предатель. Заместителей не менее $3m$, а предателей среди них - не более $m-1$, поэтому по предположению индукции протокол $BG(m-1)$ среди заместителей обладает согласованностью. Поэтому копия приказа, пересланная каждым из заместителей коллегам, будет принята всеми одинаково. Это означает, что все честные заместители получат одно и то же представление о приказах, полученных другими заместителями. Это, в свою очередь, означает, что у честных заместителей будет совпадать «сводка приказов». Но в этом случае они все примут одинаковое решение.

Доказательство завершено.

Как мы видим, построенный нами протокол работает и отвечает всем требованиям при соблюдении приведенных выше условий (менее трети предателей). Можно доказать, что для случая, когда предателей не менее трети, протокол такого вида невозможен. Это доказательство сводится к уже рассмотренному случаю «один из трех».

Как легко видеть, протокол довольно громоздок. Можно доказать, что при фиксированном m число сообщений в протоколе $BG(m)$ асимптотически равно n^{m+1} (в случае командира и заместителей) или n^{m+2} (в случае генералов) при большом n.

В конце конспекта приведено два примера для $n = 4$, $m = 1$.

3 Покер по телефону

3.1 Требования к протоколу

Итак, второй нашей задачей было изучить возможность сыграть партию в карты по телефону. Основной трудностью здесь, конечно, является раздача карт. Мы предъявим к ней вполне очевидные требования:

- Раздача должна быть случайной.
- Карты игроков не должны пересекаться.
- Игрок не должен иметь возможности узнать что-либо о картах других игроков, кроме того, что у них другие карты, чем у него.

- Должна быть возможность по ходу партии добирать карты.
- Должна быть возможность в конце партии проверить честность игроков.

3.2 Невозможность

Предположим, что мы придумали такой протокол. Ясно, что раздача карт должна представлять собой обмен сообщениями $M_1, M_2, \ldots, M_n$ между Алисой и Бобом, при этом у них обоих может быть своя секретная информация (например, закрытый ключ шифрования) R_A и R_B. Тогда результат раздачи должен быть представлен как функция $f_A(R_A, M_1, \ldots, M_n)$ для Алисы и $f_B(R_B, M_1, \ldots, M_n)$ для Боба. Для возможности проверки честности функции f_A, f_B должны быть заранее оговорены обоими игроками.

Предположим, что в игре всего три карты $\{X, Y, Z\}$, и в результате раздачи Алисе достался X, а Бобу Y. Заметим, что существует такое R'_A, что $f_A(R'_A, M_1, \ldots, M_n) = Z$ - иначе Боб по известным ему сообщениям M_k и по тому, что у него карта Y, мог бы догадаться, что у Алисы Z. Однако из тех же соображений существует такое R'_B, что $f_B(R'_B, M_1, \ldots, M_n) = Z$. Таким образом, если Алиса и Боб одновременно задумают R'_A и R'_B соответственно, то оба получат карту Z, что явно противоречит условию о непересекаемости карт.

Это доказывает принципиальную невозможность требуемого протокола.

3.3 Предъявление

Однако сейчас мы предъявим протокол, с помощью которого можно играть в карты по телефону. Для этого нам потребуется понятие коммутативного шифрования.

Вот задача на сообразительность. Пусть на одном берегу реки стоит Алиса, которая проиграла Бобу в карты по телефону большой алмаз. Боб, естественно, стоит на другом берегу. Единственное средство сообщения между ними - паром со встроенным в него сейфом без замка. Причем паромщик уже жадно заглядывается на алмаз в руках Алисы. Однако по счастливой случайности у Алисы и Боба есть по навесному замку с ключом (у каждого свой). Как переправить алмаз, не дав паромщику шанса его присвоить?

Ответ прост: Алиса кладет алмаз в сейф, запирает его на замок и отправляет Бобу. Боб не пытается взломать сейф, а вместо этого навешивает рядом с алисиным замком свой и отправляет паром к Алисе. Алиса, увидев, что сейф закрыт на замок Боба, снимает свой замок и отправляет сейф обратно. Боб, наконец, снимает свой замок и забирает желанный алмаз.

Вполне возможно, что именно эта задачка послужила отправной точкой при создании методов коммутативного шифрования. Здесь важно, что замки на сейф можно навешивать и снимать *независимо друг от друга*. Точно так же, если имеются две криптосистемы E_1 и E_2 (функции, сопоставляющие

исходному сообщению шифрованное), обладающие свойством $E_1 \circ E_2 = E_2 \circ E_1$, то такие системы называются *коммутирующими*.

Примером таких систем могут служить две системы RSA по одинаковому модулю, так как $(t^{e_1})^{e_2} = (t^{e_2})^{e_1}$.

Итак, вот наш протокол для игры в покер.

1. Алиса и Боб тайно друг от друга выбирают две коммутирующие криптосистемы.
2. Алиса зашифровывает своим ключом все 52 карты, перемешивает их и отправляет шифрограммы Бобу.
3. Боб случайным образом выбирает из них 5 шифрограмм для Алисы и отправляет их ей.
4. Алиса с помощью своей криптосистемы расшифровывает свои карты.
5. Боб случайным образом выбирает из оставшихся шифрограмм 5 для себя, зашифровывает их своим ключом и отправляет Алисе.
6. Алиса расшифровывает их своим ключом и отправляет их Бобу.
7. Боб окончательно расшифровывает свои карты своим ключом.
8. Если игрокам потребуется добрать карты из колоды, применяется аналогичная последовательность действий.

Этот протокол, казалось бы, хорош. Боб не знает, какие карты у Алисы, поскольку он видел только шифрограммы, зашифрованные алисиным ключом. Алиса не знает, какие карты у Боба, поскольку она видела только шифрограммы, зашифрованные ключом Боба. Но это все в идеале. К сожалению, требование коммутативности систем накладывает сильные ограничения на их выбор. Например, если мы пользуемся RSA (ключ Алисы - a, Боба - b), то для каждой карты Боба t Бобу известны t^b (он получает их от Алисы перед тем, как окончательно расшифровать), t^{ab} (он отправляет их Алисе) и t^a (он получает их от Алисы). При достаточной вычислительной мощности Боб может решить проблему дискретного логарифма и взломать код Алисы со всеми вытекающими последствиями.

Именно поэтому между второй и третьей частями этой главы нет противоречия. Абсолютно надежный протокол невозможен, зато возможен криптографически надежный.

4 Пример работы византийского протокола

Пусть $n = 4$, $m = 1$. Может быть два принципиально различных случая: когда предатель - командир и когда предатель - один из заместителей.

Командир. Желая ослабить наступление, командир приказывает двум заместителям атаковать, а третьему - отступать. Согласно протоколу $BG(1)$, заместители рассылают друг другу копии приказа, используя протокол $BG(0)$, то есть, посылают их прямым текстом. В итоге первый заместитель получает следующую сводку:

Командир	Атаковать!
Второй зам.	Командир приказал атаковать!
Третий зам.	Командир приказал отступать!

Согласно $BG(1)$, первому заместителю следует атаковать. Аналогичная ситуация складывается у второго заместителя. А вот сводка для третьего:

Командир	Отступать!
Первый зам.	Командир приказал атаковать!
Второй зам.	Командир приказал атаковать!

Таким образом, третий заместитель тоже будет атаковать, несмотря на преступный приказ командира, и тем самым обеспечит согласованность.

Заместитель. Пусть предателем является третий заместитель. Желая запутать остальных, он говорит, что командир приказал ему отступать, когда на самом деле приказ был атаковать. В таком случае первый заместитель получает следующую сводку:

Командир	Атаковать!
Второй зам.	Командир приказал атаковать!
Третий зам.	Командир приказал отступать!

Сводка второго заместителя будет выглядеть так же. Как мы видим, гнусному предателю не удалось запутать доблестных воинов, которые смело пойдут в атаку.

Было бы интереснее, конечно, привести протокол $BG(2)$, но он, как известно, работает при $n \geq 7$, так что в нем участвует не менее 156 сообщений.