Дисциплина СВ3.03 Криптографические протоколы

по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем

Практика 1.

Протокол Византийского соглашения

Протокол византийского соглашения

byzantine agreement

Протокол решения следующей задачи, формулируемой традиционно на историческом примере армии Византийской империи периода упадка (задача о византийских генералах). Имеются $n+1$ участник — главнокомандующий и n генералов. Главнокомандующий посылает каждому генералу приказ, который имеет всего два возможных варианта: атаковать или отступать. Часть генералов, в т. ч. и главнокомандующий, могут оказаться предателями. Честные генералы, обмениваясь сообщениями по каналам связи (которые обычно предполагаются защищенными) должны достигнуть соглашения о единых действиях — атаковать или отступать. Нетривиальной задачу делает следующее требование: если главнокомандующий честный, то все честные генералы обязаны выполнить его приказ.

Протокол византийского соглашения является базовым для построения многих других протоколов: достижения консенсуса, частичного соглашения гарантированной широковещательной рассылки

Задание и контрольные вопросы

1. **Изучить протокол.**
2. **Условие завершения?**
3. **Условие корректности?**
4. **Изучить «Облака и византийские генералы»**
5. **Придумать как он может быть использован.**
6. **Разработать программу для иллюстрации (в минимальном варианте в виде презентации).**
7. **Какие модели разработки протоколов существуют?**
8. **Протокол может состоять из многих раундов обмена сообщениями между P и V и должен удовлетворять двум условиям . Перечислите и поясните эти условия.**
9. **Привести примеры практического применения теории доказательств с нулевым разглашением.**

Задача византийских генералов

- **Задача византийских генералов** — в криптологии задача взаимодействия нескольких удаленных абонентов, которые получили приказы из одного центра. Часть абонентов, включая центр, могут быть противниками. Нужно выработать единую стратегию действий, которая будет выигрышной для абонентов.
- **Формулировка**
- Византия. В ночь перед великим сражением, Византийская армия содержит легионов. Каждый из них подчиняется своему генералу. У всей византийской армии есть главнокомандующий, руководящий генералами. Империя находится в упадке и среди генералов, включая главнокомандующего, могут быть предатели. В течение всей ночи, каждый из генералов получает от предводителя приказ о действии на утро. Это может быть один из двух вариантов «атаковать» или «отступать». Если все честные генералы атакуют — они одержат победу. Если все отступят — им удастся сохранить армию. Если часть атакуют, а часть отступят — они терпят поражение. Если главнокомандующий предатель, он может дать разным генералам разные приказы, следовательно, его приказы не стоит выполнять беспрекословно. Если же каждый генерал будет действовать независимо от других, результаты битвы также могут быть плачевными. Поэтому генералы нуждаются в обмене информацией друг с другом, чтобы прийти к соглашению.

- «синих» генералов возглавляют армии в горах и готовятся атаковать «зелёных» в долине. Для связи атакующие используют надёжную связь (например, телефон). Однако из генералов являются предателями и активно пытаются воспрепятствовать согласию лояльных генералов. Согласие состоит в том, чтобы все лояльные генералы узнали о численности всех лояльных армий и пришли к одинаковым выводам (пусть и ложным) относительно состояния предательских армий. (Последнее условие важно, если генералы на основании полученных данных планируют выработать стратегию и необходимо, чтобы все генералы выработали одинаковую стратегию.)

- Каждый из лояльных генералов должен получить вектор длины n, в котором i-й элемент либо обязательно содержит численность i-й армии (если её командир лоялен), либо может содержать произвольное число, если её командир не лоялен. При этом векторы у всех лояльных командиров должны быть полностью одинаковы.

Алгоритм Лесли Лампорта

- Рекурсивный алгоритм был предложен в 1982 г. Лесли Лампортом. Алгоритм сводит задачу для случая m предателей среди n генералов к случаю m-1 предателя.
- Для случая m=0 алгоритм тривиален, поэтому проиллюстрируем его для случая n=4 и m=1 . В этом случае алгоритм осуществляется в 4 шага.
- *1-й шаг.* Каждый генерал посылает всем остальным сообщение, в котором указывает численность своей армии. Лояльные генералы указывают истинное количество, а предатели могут указывать различные числа в разных сообщениях. Генерал 1 указал число 1 (одна тысяча воинов), генерал 2 указал число 2, генерал 3 (предатель) указал трём остальным генералам соответственно x ,y ,z , а генерал 4 указал 4.
- *2-й шаг*. Каждый формирует свой вектор из имеющейся информации.
- Получается:
- Вектор 1 (1,2,x,4);
- Вектор 2 (1,2,y,4);
- Вектор 3 (1,2,3,4);
- Вектор 4 (1,2,z,4).

Алгоритм Лесли Лампорта

3-й шаг. **Каждый посылает свой вектор всем остальным (генерал 3 посылает опять произвольные значения).**

После этого у каждого генерала есть по четыре вектора:

g1	g2	g3	g4
(1,2,x,4)	(1,2,x,4)	(1,2,x,4)	(1,2,x,4)
(1,2,y,4)	(1,2,y,4)	(1,2,y,4)	(1,2,y,4)
(a,b,c,d)	(e,f,g,h)	(1,2,3,4)	(i,j,k,l)
(1,2,z,4)	(1,2,z,4)	(1,2,z,4)	(1,2,z,4)

4-й шаг. **Каждый генерал определяет для себя размер каждой армии. Чтобы определить размер -й армии, каждый генерал берёт три числа — размеры этой армии, пришедшие от всех командиров, кроме командира -й армии. Если какое-то значение повторяется среди этих трех чисел как минимум дважды, то оно помещается в результирующий вектор, иначе соответствующий элемент результирующего вектора помечается неизвестным (или нулём и т. п.).**

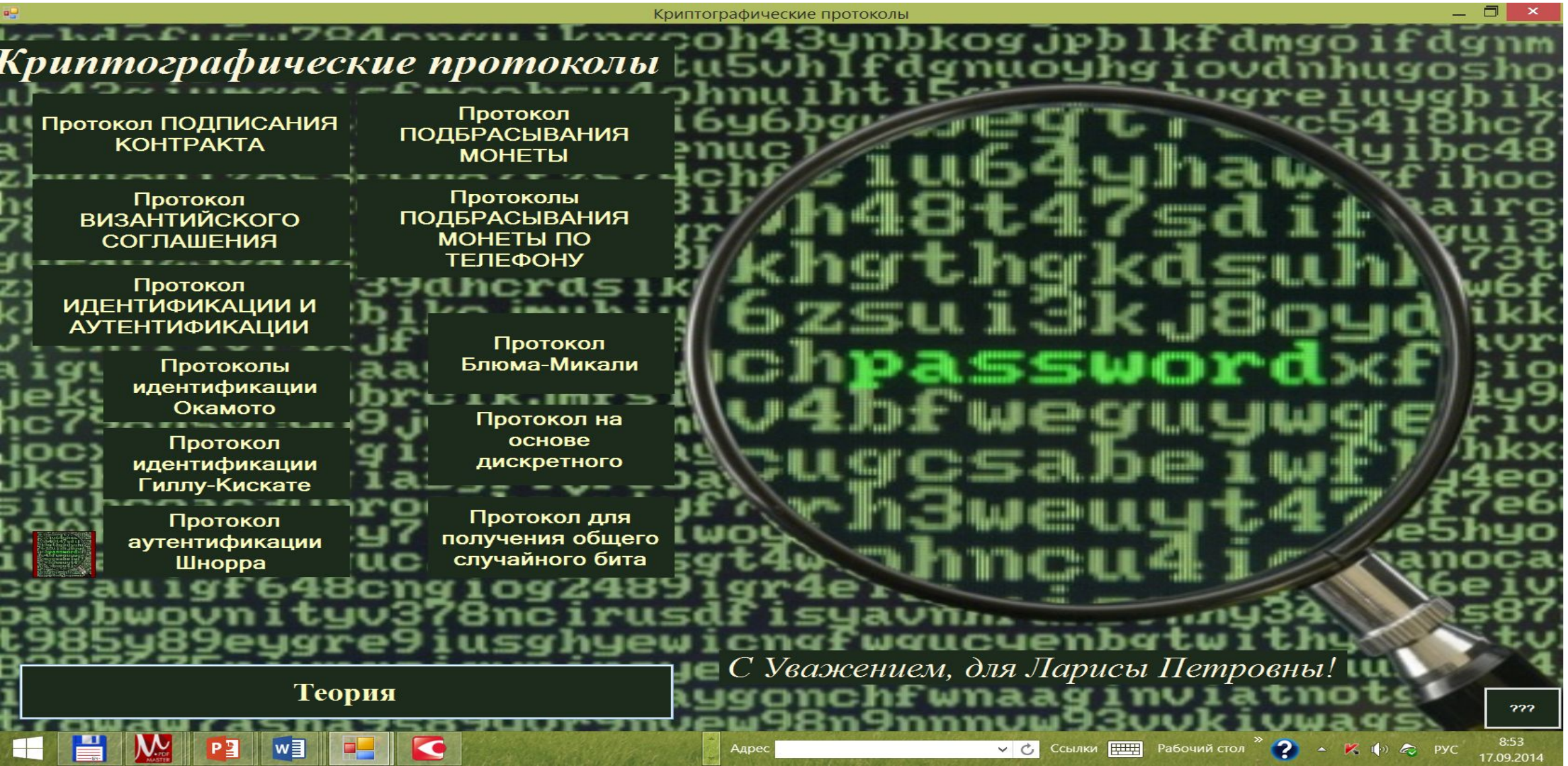
Все лояльные генералы получают один вектор , где есть число, которое встречается как минимум два раза среди значений , или «неизвестность», если все три числа различны. Поскольку значения и функция у всех лояльных генералов одни и те же, то согласие достигнуто.

Алгоритм Лесли Лампорта

- *4-й шаг.* Каждый генерал определяет для себя размер каждой армии. Чтобы определить размер -й армии, каждый генерал берёт три числа — размеры этой армии, пришедшие от всех командиров, кроме командира -й армии. Если какое-то значение повторяется среди этих трех чисел как минимум дважды, то оно помещается в результирующий вектор, иначе соответствующий элемент результирующего вектора помечается неизвестным (или нулём и т. п.).

  Все лояльные генералы получают один вектор (1,2,f(x,y,z),4) , где f(x,y,z) есть число, которое встречается как минимум два раза среди значений (x,y,z) , или «неизвестность», если все три числа (x,y,z) различны. Поскольку значения x,y,z и функция f у всех лояльных генералов одни и те же, то согласие достигнуто.

Запустить программу и изучить протокол византийского соглашения



Византийские генералы

Общая картина:

– Пусть вокруг города расположено n византийских отрядов, каждым командует свой генерал

– У каждого генерала есть некоторая информация

– Генералы могут посылать сообщения другим генералам

Среди генералов могут быть предатели

Требования:

А Все честные генералы принимают одинаковое решение

Б Малое количество предателей не способно заставить честных выбрать "плохой план"

•

План протокола

Фаза 1 Генералы делятся своими наблюдениями

Фаза 2 Генералы принимают решение

Требования к первой фазе:

- 1А Наблюдения честных генералов до других честных генералов дойдут неискаженными
- 1Б От нечестного генерала все честные генералы получат одинаковое наблюдение

Анализ плана:

Все честные генералы получат одинаковую сводку

Фаза 1 Генералы делятся своими наблюдениями

Фаза 2 Генералы принимают решение

- Все честные генералы получат одинаковую сводку
- Наблюдения всех честных генералов будут поняты правильно Генералы смогут принять одинаковый и "хороший" план
-

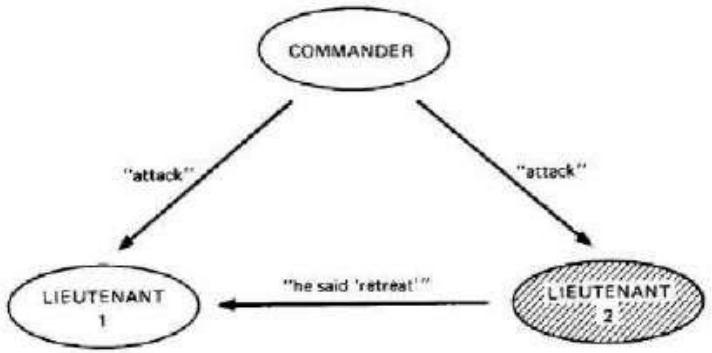
ЗАДАЧА О ВИЗАНТИИСКИХ ГЕНЕРАЛАХ

Командир должен передать свой приказ $n - 1$ лейтинанту так, чтобы были выполнены два свойства:

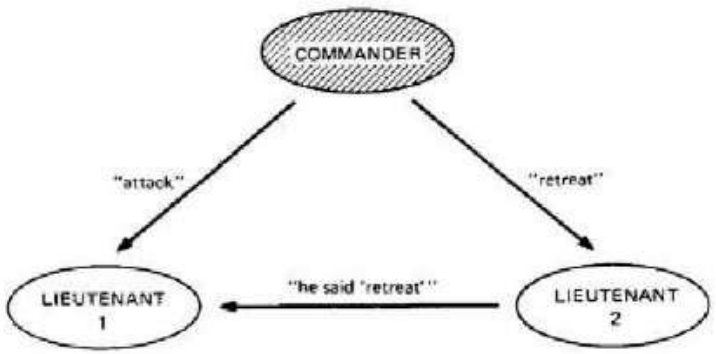
Согласованность Все генералы получат одинаковый приказ

Исполнительность Если командир честен, то приказ будет совпадать с исходным

Кстати, а почему генералы — византийские?

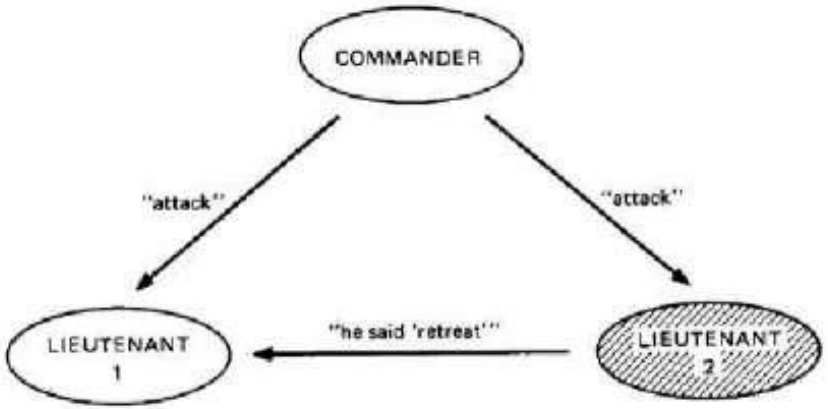


Пусть Командир честен и говорит “атакуй”, а Лейтенант 2 ведет себя, как будто ему сказали “отступай”.
Следуя **исполнительности**, Лейтенант 1 обязан атаковать

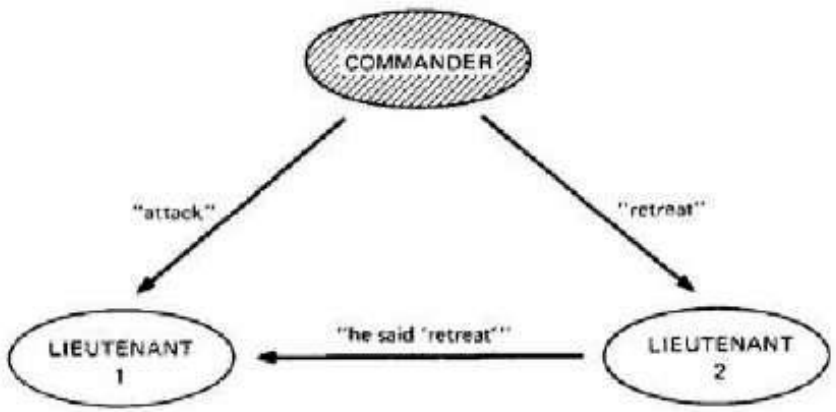


Пусть теперь Командир — предатель. Он говорит Лейтенанту 1 “атаковать”, а Лейтенанту 2 “отступать”.
С точки зрения Лейтенанта 2 эти ситуации не отличаются, так что он вынужден атаковать

Невозможность “один из трех”



Пусть Командир честен и говорит “атакуй”, а Лейтенант 2 ведет себя, как будто ему сказали “отступай”.
Следуя **исполнительности**, Лейтенант 1 обязан атаковать



Пусть теперь Командир — предатель. Он говорит Лейтенанту 1 “атаковать”, а Лейтенанту 2 “отступать”.
С точки зрения Лейтенанта 2 эти ситуации не отличаются, так что он вынужден атаковать

Но Лейтенант 2 (из симметрии) будет отступать!
Противоречие с согласованностью.

Протокол $BG(0)$:

1. Командир рассылает всем свой приказ
2. Лейтенанты принимают этот приказ в качестве окончательного

Протокол $BG(m)$:

1. Командир рассылает всем свой приказ
2. Для каждого i Лейтенант i рассылает остальным лейтенантам полученный им приказ с помощью $BG(m-1)$
3. В качестве окончательного решения лейтенанты выбирают наиболее частое значение среди своего командирского приказа и $n-2$ значений полученных с помощью $BG(m-1)$ от других лейтенантов

Исполнительность: Командир честен $\Rightarrow$ получен исходный прика

Лемма об исполнительности

Для всех k и m алгоритм $BG(m)$ обладает исполнительностью для хотя бы $2k + m + 1$ генералов, среди которых не более k предателей.

Доказательство.

Индукция по m. При $m = 0$ верно!

Переход. Каждый честный генерал пользуется $BG(m-1)$ среди $\geq 2k + m - 1$ генералов и не более k предателей. Т.е. по предположению "исполнительность" выполнена. Таким образом все честные генералы получат хотя бы $k + m$ копий верного приказа, а значит выполнят его. $\square$

Корректность протокола

Протокол $BG(m)$ обладает исполнительностью и согласованностью для $\geq (3m+1)$ офицеров и $\leq m$ предателей.

Доказательство.

Исполнительность доказана в Лемме ($k := m$)

Индуция по m. База $m = 0$ верно!

Переход. Если командир не предатель, из исполнительности следует согласованность.

Пусть командир — предатель. Тогда по индукции $BG(m-1)$ обладает согласованностью (у нас $3m$ офицеров и не более $m-1$ предателя).

Следовательно все честные генералы получат одинаковые наборы из n значений, и сделают одинаковый окончательный выбор. Согласованность доказана. □

Протокол византийского соглашения

- Протокол решения данной задачи называется протоколом византийского соглашения (byzantine agreement.) При византийских соглашениях или при реализации протокола византийских соглашений для любого начального входа xi, i∈[1,...,n] участника i и некоторого параметра d (соглашения) должны быть выполнены следующие условия:
- 1. Условие завершения. Все честные участники вычислений в конце протокола принимают значение d.
- 2. Условие корректности. Если существует значение x такое, что для честных участников xi=x, тогда d=x.
- «Задача византийского соглашения» формулируется на основе «задачи о византийских генералах»: для n взаимодействующих генералов нужно предложить такой протокол взаимодействия, чтобы при наличии среди них m «нелояльных» генералов остальные генералы – «лояльные», – имея каждый свое мнение, всегда вырабатывали согласованную общую позицию (например, штурмовать крепость или нет). В протоколе все генералы по очереди выступают в роли командующего, они рассылают свое мнение и собирают мнения остальных в роли подчиненного. В этом заключается принцип решения даной задачи. Все честные генералы получают в итоге одинаковый результат, это гарантирует процедура голосования по мажоритарному принципу. При пересылке подписанных и неподписанных сообщений, способы решения задачи различны.
- На протоколе византийского соглашения базируется построение большого количества других протоколов: достижения консенсуса, частичного соглашения гарантированной широковещательной рассылки и др. Каждый год появляется большое количество новых протоколов, которые решают еще более сложные задачи защиты распределенных систем.
- Таким образом, недавно был предложен новый метод обнаружения «лжецов», квантовый. Он является вариантом «Византийского соглашения».
- Пример этой схемы: Соглашение нескольких генералов, некоторые из них подкуплены, о необходимости атаковать вместе или отступить. Цель противника: отступление части генералов, для успешной победы

Схема «Византийского соглашения» с использованием квантовых коммуникаций

- Схема «Византийского соглашения» с использованием квантовых коммуникаций была предложена группой ученых из разных научных учреждений. Они написали статью, которая называется "Experimental Demonstration of a Quantum Protocol for Byzantine Agreement and Liar Detection" ("Экспериментальная демонстрация квантового протокола Византийского соглашения и обнаружения лжеца"), которая была опубликована в Physical Review Letters.
- Этот протокол дает возможность найти согласованное решение и определить возможного «лжеца» из трех участников, которые обмениваются сообщениями. Так же как и любое другое «Византийское соглашение», можно сказать, что этот протокол сводится к обеспечению:
- 1. Все участники получают один и тот же план
- 2. У плана есть определенный автор, и если он незлонамеренен, то все соглашаются с ним и следуют его плану.
- Для того чтобы успешно реализовать «Византийского соглашения», нужно, чтобы у всех участников были наборы чисел, которые связаны между собой, но не известны другим. Этот протокол позволяет безопасную генерацию и дистрибуцию таких чисел и обнаружение «лжеца» с помощью квантовых каналов связи.
- Чаще всего, сложность реализации квантовых протоколов между более чем двумя участниками заключается в необходимости использования кутритов. Трудно контролировать физические носители кутритов, например, сложно реализовывать из передачу. Но исследователи смогла не использовать кутриты, и вместо них использовала в качестве носителей кубитов четыре поляризованных фотона. Исследователи задействовали фотоны, которые находятся в запутанном квантовом состоянии. Иначе говоря, фотоны имеют коррелированные квантовые свойства после

Предложен квантовый метод обнаружения «лжецов»

http://rnns.ru/5175-predlozhen-kvantovyjj-metod.html

В 1985-1986 гг., понимание различных протоколов и способов их построения привело к появлению двух значимых математических моделей - интерактивной системы доказательства и доказательства с нулевым разглашением. Исследования этих моделей позволило доказать некоторые утверждения, которые играют важную роль при разработке криптографических протоколов. Интерактивная система доказательства (P, V, S) - протокол взаимодействия двух абонентов: P (доказывающий) и V (проверяющий). Абонент P хочет доказать V, что утверждение S истинно. При этом абонент V самостоятельно, без помощи P, не может доказать утверждение S (поэтому V и называется проверяющим). Абонент P может быть и противником, который хочет доказать V, что утверждение S истинно, хотя оно ложно. Протокол может состоять из многих раундов обмена сообщениями между P и V и должен удовлетворять двум условиям:

1) полнота — если S действительно истинно, то абонент P почти наверняка убедит абонента V признать это;

2) корректность — если S ложно, то абонент P вряд ли убедит абонента V, что S истинно.

В определении системы (P, V, S) не допускалось, что V может быть противником. В случае, если V оказался противником, который хочет получить от P новую информацию об утверждении S, P, естественно, может не хотеть, чтобы это случилось в результате работы протокола (P, V,S). Протокол (P, V, S), который решает такую задачу, называется доказательством с нулевым разглашением. Он должен удовлетворять еще одному условию:

3) нулевое разглашение (или стойкость) — в результате работы протокола (P, V, S) абонент V не увеличит свои знания об утверждении S или, другими словами, не сможет извлечь никакой информации о том, почему S истинно.

В 1991 году для большого класса математических проблем (включающего так называемые NP-полные задачи) получилось доказать существование доказательств с нулевым разглашением. Но это доказано только в предположении, что существует односторонняя функция.

«Интеллектуальные карточки» (кредитные карточки, не подделываемые удостоверения и т. п.) - практическое применение теории доказательств с нулевым разглашением. В них есть микропроцессор, который реализует действия участника P в протоколе, который претендует быть протоколом

Задание и контрольные вопросы

1. Изучить протокол.
2. Условие завершения?
3. Условие корректности?
4. Изучить «Облака и византийские генералы»
5. Придумать как он может быть использован.
6. Разработать программу для иллюстрации (в минимальном варианте в виде презентации).
7. Какие модели разработки протоколов существуют?
8. Протокол может состоять из многих раундов обмена сообщениями между P и V и должен удовлетворять двум условиям . Перечислите и поясните эти условия.
9. Привести примеры практического применения теории доказательств с нулевым разглашением.