РЕФЕРАТ

НА ТЕМУ

ZERO KNOWLEDGE PROOFS

ДОКОЗАТЕЛЬСТВА С НУЛЕВЫМ ЗНАНИЕМ

работу выполнили:

ученики 10а класса

ГОЛИКОВ АНДРЕЙ

СИРОКЛИН ВАЛЕНТИН

1998 год

В наше время при таком количестве электроники в мире очень важно создать систему шифровки которую нельзя подделать. Старые способы шифрования не подходят так как шифр может попасть в чужие руки или может быть «взломан» компьютером.

Поэтому своевременно и очень перспективно появления метода Zero Knowledge Proofs (доказательства с нулевым знанием) позволяющий создать систему шифровки которая с данной точностью подтверждает что человек тот за кого он себя выдает и не дает никакой информации которую можно использовать другому человеку.

Метод ZKP основан на том что проверяющий знает всегда только половину информации. Конечно при таком условии нельзя быть уверенным в том что человек тот за кого он себя выдает. Но проверяющий каждый раз может спросить любую часть информации причем несколько раз.

Рассмотрим данный метод на примере графов. Граф- конечная совокупность точек, называемых вершинами; некоторые из них соединены друг с другом линиями, называемыми ребрами графа. Простейший вид графа - это города соединенные дорогами на карте.

У каждого графа с количеством точек больше двух есть гамильтонов цикл- это способ соединения всех вершин графа одной кривой, проходящий по его ребрам и не проходящий через одну вершину два раза. Допустим проверяющему показали гамильтонов цикл графа но он не знает от какой точки к какой идти, если проверяющий убедился в том что у проверяемого нужный граф то он не видит гамильтонов цикл так как у графа изменились координаты точек.

Каждый вопрос будет понижать шансы на случайный ответ. С начало вероятность угадать равна 1/2, потом 1/4 и через сто вопросов вероятность упадет до 1/2100 . Согласитесь что если человек не знает правильного графа и гамильтонова цикла то ему будет затруднительно ответить чтобы хоть раз не ошибиться, а проверка заканчивается при первой же ошибке.

Как происходит проверка. Допустим Алису проверяет Боб. У Алисы есть граф для которого как она утверждает знает гамильтонов цикл.

Сначала Алиса приходит к Бобу с графом у которого закрыты узлы монетами. Она спрашивает боба что ему показать: Гамильтонов цикл или узлы графа. Боб бросает монету и говорит покажи мне узлы, Алиса снимает монеты и Боб видит что действительно Каждая точка графа которая обязательно должна иметь название соединена с другой так как у боба на проверочном графе.

Боб говорит ты просто знала что я спрошу. Тогда Алиса отворачивается меняет расположение точек в пространстве снова их закрывает поворачивается и опять спрашивает Боба что ему показать. Боб опять бросает монету и на этот раз говорит покажи мне гамильтонов цикл Алиса соединяет все точки графа друг с другом не проходя по ним два раза. Боб убеждается что Алиса действительно знает гамильтонов цикл для данного графа но не знает название точки от какой Алиса проводит кривую. Таким образом Спросив Алису сто раз Боб убеждается что она действительно та за кого себя выдает. При этом Боб так и не узнал Гамильтонов цикл для данного графа так как не знал последовательность точек которые надо соединять а гамильтонов цикл найти для граф с десятью вершинами уже не просто, а если у графа 100 вершин то это уже почти невозможно. А если вершин 1000 то подбор гамильтонова цикла на современном компьютере займет несколько сотен лет.

Перед Алисой встает таже задача по нахождению гамильтонова цикла для своего графа. Алиса решает эту задачу так: Алиса рисует любую запутанную кривую в точках перигиба кривой Алиса расставляет точки графа. Потом между данными точками проводит еще несколько ребер графа чтоб усложнить его. И получает достаточно сложный граф для которого она знает гамильтонов цикл. Данный граф передают проверяющему не говоря ему гамильтонов цикл.

Чтоб показать вам всю сложность нахождения гамильтонова цикла рассмотрим граф из семи точек, приведенный на рисунке ниже. Если попытаться самому придумать гамильтонов цикл то на это уйдет от 30 минут до нескольких часов.



На рисунке показан граф с 7 вершинами; сплошные линии- гамильтонов цикл для данного графа пунктир ребра по которым не прошла кривая гамильтонова цикла.

В качестве Боба и Алисы могут выступать компьютер и пластиковая карточка типа той которая сейчас служит для банковских расчетов. Даже если человек сможет подключится к проверяющему компьютеру то он все равно не сможет узнать гамильтонов цикл для графа находящегося на карточке.

Метод ZKP может использоваться не только для примера с графами но и на многих других примерах, просто в данном случае легче всего объяснить в чем суть метода ZKP. Хоть и явны видны преимущества данного вида кодировки нельзя забывать и про систему (PASSWORD)овых шифровок так как если охраняется не очень важный объект то проще и быстрее проверять (PASSWORD) чем проводить проверку методом ZKP.

Мы попробовали пройти систему кодировки ZKP.

Для примера мы разобрали разные фрагменты графов что бы найти закономерность в построении гамильтонова цикла .Мы можем найти алгоритм построения гамильтонова цикла на данных фрагментах, что бы в дальнейшем строить этот цикл на более сложных графах.

Пример1.

A A E D C B F S N P G A

В данном графе легко можно B построить гамильтонов цикл

F G E так как в данном графе есть два

S P контура , которые находятся

N друг в друге и соединены точками.

C D Таким образом построение данного графа является самим гамильтоновым циклом и практически все графы строятся на основе самого гамильтонова цикла. С добавлением других ребер.

Гамильтонов цикл легко искать если граф имеет вид замкнутых контуров соединенных более чем через две точки друг с другом

Пример 2.

На данном графе намного сложнее построить гамильтонов цикл так как не все точки соединены с друг другом

А Гамильтонов цикл:

Б Л Д Б А Л К В С Е Д

Д Е В данном случае мы нашли

С его за 7 минут 34 секунды

В К и если бы точки Б и В не лежали бы рядом то, это заняло бы у нас намного больше времени. Граф не обязательно должен быть таким , главное что граф может растягиваться как угодно ,и точки могут менять свои координаты, главное что бы A соединялось с

Б Д Л и тд.

Пример 3.

Мы можем разбивать сложные графы на более простые, гамильтонов цикл которых нам известен .Покажем это на примере ранее рассмотренных графов.

А A1

B H B1 H1 G R1 T1

E F E1 Y1

C D

1. C1 F1

2. D1

Мы можем пройти цикл 1. и можем пройти цикл 2.А если представить что у нас есть цикл из 1 и 2 когда соединены H и B1, C и D1, то мы можем его пройти его как первый если уверены что можем пройти от B1 до C1 по всем точкам , а так как это легко ( B1 R1 A1 T1 H1 Y1 D1 F1 E1 C1) и следовательно мы можем составить для него гамильтонов цикл и таким же образом мы можем составить гамильтонов цикл для многих сложных графов, правда с затратой времени , главное найти начальную (конечную) точку и несколько графов , по которым можно

пройти так же легко как и по графу в примере .

CHECKING PROGRAM

Checking program – разновидность верификации , но эта на много удобнее и дешевле . СHEKING PROGRAM заключается в том , что команды , которые посылает программа проходят через специально сделанную внутреннюю программу , которая настроена на новую версию, и она просто изменяет те команды, которые не подходят для данной версии.

При изготовлении ракеты надо делать для нее специальную программу, но если раньше такая программа уже была сделана для похожей ракеты, а теперь появились маленькие изменения, то CHECKING PROGRAM будет пропуская через себя команды изменять их, если эта команда не изменена, и не будет изменять если данная команда не требует изменения , таким образом CHECKING PROGRAM экономит время и деньги.

Если человек обладает такими навыками то он может зарабатывать на составлении таких программ неплохие деньги.