Протоколы аутентификации, обладающие свойством доказательства с нулевым разглашением (Zero – Knowledge protocols).

Дроздов Константин, группа 015

1. Введение.

Протоколы аутентификации, обладающие доказательством с нулевым разглашением (далее ZK протоколы) позволяют произвести процедуры идентификации, обмена ключами и другие основные криптографические операции без утечки любой секретной информации в течение информационного обмена. Этой цели можно добиться при помощи демонстрации знания секрета, однако проверяющий должен быть лишен возможности получать дополнительную информацию о секрете. То есть, ZK протоколы позволяют установить истинность утверждения, не передавая какой-либо дополнительной информации о самом утверждении.

ZK – протоколы являются системой интерактивного доказательства, в которой проверяющий и доказывающий обмениваются многочисленными запросами и ответами. Целью доказывающего является убеждение проверяющего в истинности утверждения. Поверяющий отклоняет или принимает доказательство. Таким образом, ZK протоколы носят вероятностный, а не абсолютный характер.

Сторона A владеет секретом s и пытается убедить сторону B в знании секрета. Стоит отметить, что доказательство знания секрета отличается от доказательства того факта, что секрет существует.

2. Характеристики ZK протокола

ZK протоколы могут быть описаны как криптографические протоколы обладающие следующими свойствами:

1. **Проверяющий не может ничего узнать из протокола.**
2. **Доказывающая сторона не может обмануть проверяющую сторону.**
   Если сторона A не знает секрета s и пытается доказать стороне B его знание, то после нескольких раундов протокола данный факт может быть установлен на столько точно, на сколько это необходимо
   Протокол также является “Cut AND Choose”, то есть после первого неудачного раунда сторона B точно знает, что A не легальна
3. **Проверяющая сторона не может обмануть Доказывающую сторону.**
   Сторона B не может вынести из протокола какой либо информации, даже если она не следует протоколу. Единственное что может сделать сторона B, это убедить себя, что сторона A знает секрет. Доказывающая сторона всегда раскрывает только одно из многих решений любой поставленной проблемы, и никогда все, что позволило бы найти сам секрет.
4. **Проверяющая сторона не может стать доказывающей для любой третьей стороны.**

3. Режимы Работы протокола.

Существует три основных режима работы ZK протокола
Интерактивный, когда стороны A и B интерактивно взаимодействуют через протокол, шаг за шагом проверяя достоверность.
Параллельный , когда сторона A формулирует ряд запросов, а сторона B в это время запрашивает ряд ответов на поставленные задачи. Данный режим может быть использован, чтобы снизить количество интерактивно передаваемых сообщений при плохом уровне связи.
Автономный (Offline), когда сторона A формулирует ряд запросов, затем, играя роль стороны B, использует криптографически стойкую однонаправленную хеш функцию набора, чтобы выбрать произвольное решения для каждого запроса. После этого A добавляет ряд полученных решений к сообщению. Этот режим может быть использован для цифровой подписи.

4. Теория и примеры ZK протоколов.

Подобно остальным криптографическим протоколам, ZK основан на обычной криптоматематике, такой как: вычисления по модулю, дискретная математика, операции над большими целыми числами (сотни, тысячи бит).

Стойкость ZK протокола основана на трудно решаемых задачах, таких как:

А. Вычисление дискретного логарифма.
Б. Факторизация больших чисел.

Рассмотрим некоторые существующие ZK протоколы, основные идеи и способы их работы.

4.1 Доказательство знания

Если сторона A имеет хорошие шансы убедить сторону B, то она может вычислить секрет, исходя из которого знание будет доказано**.**
Хорошим примером доказательства знания является пример “пещера” **[3]**.
Имеется U образная пещера, разделенная по середине дверью. Дверь открывается с помощью секретного пароля. Сторона A пытается убедить B в знании пароля.
Механизм действия следующий:

A. A заходит в любую ветвь пещеры, неизвестную B.
B. B просит A выйти из произвольно выбранной ветви (левой или правой).
C. Если A знает секретный пароль, она может в любой момент выйти из указанной ветви пещеры. Иначе положительный исход будет иметь вероятность 50%.

Таким образом, после одного раунда протокола с вероятностью 50% можно утверждать, что A знает пароль. B может провести столько раундов, сколько

необходимо. (После 10 раундов вероятность, что А не знает пароля составит 1/1024).

4.2 Идентификация, протокол Фиата-Шамира.

Это один из наиболее известных ZK протоколов идентификации. Схема его работы следующая. А доказывает В знание секрета s за t раундов по три сообщения в каждом.
Параметры протокола:

- Доверительный центр Т выбирает и публикует модуль n (512-1024бита), являющийся произведением двух больших чисел (n=p*q, p и q сохраняются в секрете).
- Каждый доказывающий выбирает секрет s взаимно простой с n , 1<= s<=n-1, вычисляет v = s^2 mod n и регистрирует v у Т в качестве своего открытого ключа.

Сообщения, передаваемые в рамках каждого раунда:

A->B: x = r^2 mod n

A<-B: e принадлежит {0,1}

A->B: y=rs^e mod n

В принимает доказательства за t раундов , и последовательность действий в рамках протокола имеет вид:

- А выбирает случайное число r, 1<=r<=n-1 и посылает В x=r^2 mod n.
- В выбирает случайным образом e и посылает его А.
- А вычисляет y и посылает его В, где y = r(e=0) или y=rs(e=1).
- В отвергает доказательство, если y=0, иначе производится проверка

  y^2 == xv^e mod n . В зависимости от e y^2=x^2 mod n или y^2 = xv mod n , иначе v = s^2 mod n

Число раундов выбирается от 20 до 40.

4.3 Обмен ключами.

Протокол может быть разработан с помощью идентификации, основанной на RSA публичном ключе и комбинированной со свойствами ZK протоколов и обменом ключами (Для сессинного ключа). Сторона В может зашифровать произвольное число с помощью публичного ключа стороны А, и если А может расшифровать его с помощью своего секретного ключа, то А идентифицировано. Чтобы скрыть возвращаемое зашифрованное значение используется однонаправленная хеш функция. Таким образом В

может только проверить, что присланное стороной А значение соответствует хеш функции от выбранного числа. Сессионный ключ может быть помещен в некоторые биты произвольного числа, которые никогда не пересылаются в чистом виде.

4.4 Цифровая Подпись

Большинство ZK протоколов может быть использовано для цифровых подписей, если сторону В заменить криптографически стойкой однонаправленной хеш функцией. Сторона А может сформулировать ряд запросов, использовать однонаправленную хеш функцию как виртуальную строну В (которая произвольным образом потребует один ответ на каждый запрос) и предоставить эти ответы. В качестве аргументов хеш функции используются набор ответов и запросов. Таким образом, ни ответ, ни запрос не могут быть изменены без изменения подписи. Результат действия “хорошей” криптографической однонаправленной хеш функции является полностью произвольным и не предсказуемым. Принимающая сторона вычисляет значение хеш функции и проверяет корректность ответов на запросы. Если проверка пройдена, то подпись может считаться верной.

Рассмотрим в качестве примера схему ЭЦП Шнорра

Пусть p и q простые числа, такие что p делит q-1, пусть g принадлежит Zp. g^q = 1 mod p , g не равно 1. В качестве секретного ключа выбирается x принадлежащий {1,.. q-1}. Открытый ключ y=g^(-x) mod p.

- А выбирает случайное число k принадлежащее {1,..,q-1} и вычисляет r=g^k mod p;
- А вычисляет e = h(r,m), где m- подписываемое сообщение.
- А вычисляет s = (k+ex) mod q и посылает сообщение m с подписью (e,s) получателю В.
- В вычисляет r1 = g^s*y^e mod p и проверяет, выполняется ли равенство e = h(r1,m). Если да, то подпись принимается, в противном случае - отвергается.

Преимущество схемы Шнорра перед схемой Эль Гамаля заключается в том, что k выбирается из меньшего множества (длина k -- порядка 140 битов). Это повышает эффективность вычисления дискретных экспонент. Кроме того, стоит заметить, что использование в схеме Шнорра хэш-функции при вычислении e и приведение подписи s по модулю q сокращают длину подписи по сравнению со схемой Эль Гамаля. Длина подписи - один из важнейших показателей эффективности схемы.

5. Системные требования

Ниже приведена сравнительная таблица системных требований различных семейств криптопротоколов

Семейство протоколов	Размер сообщение	Количество раундов	Количество вычислений	Требования к памяти
Zero-knowledge	большой	много	большое	большая
Public-key	большой	один	очень большое	большая
Symmetric	маленький	один	маленькое	маленькая

6. Заключение

Из выше приведенного материала видно, что ZK протоколы могут применяться в системах с повышенным требованием к безопасности, но их применение предъявляет жесткие требования к вычислительным способностям и размеру памяти.

Список Литературы

[1] Zero Knowledge Protocols and Small Systems
http://www.tml.hut.fi/Opinnot/Tik-110.501/1995/zeroknowledge#features

[3] Bruce Schneier. *Applied Cryptography*, Wiley & Sons, 1994, ISBN 0-471-59756-2, 1994.

[2] Ivan Bjerre Damgård. *Zero-knowledge Protocols*, Århus University and CRYPTOMATHIC A/S.

[3] DigiCash, Inc. Zero Knowledge Interactive Proofs
http://www.digicash.com/~nick/zkip.html

[4] DigiCash publications. a list of publications by D. Chaum
http://www.digicash.com/publish/publist.html

[5] Tatu Ylqnen. crypto page
http://www.cs.hut.fi/crypto/

[6] UCL Crypto Group.
UCL Crypto Group home page
http://www.dice.ucl.ac.be/crypto/crypto.html

[7] RSA Data Security, Inc. FAQ About Today's Cryptography
http://www.rsa.com/rsalabs/faq/faq_home.html

[8] Security Papers
http://www.ccs.neu.edu/home/thigpen/html/security.html

[9] Анохин М. И., Варновский Н. П., Сидельников В. М., Ященко В. В. **Криптография в банковском деле.** Методические материалы. М.: МИФИ. 1997
http://www.cryptography.ru/db/msg.html?mid=1169307