Схема Шнорра

Материал из Википедии — свободной энциклопедии

Схема Шнорра (англ. *schnorr scheme*) — одна из наиболее эффективных и теоретически обоснованных схем аутентификации. Безопасность схемы основывается на трудности вычисления дискретных логарифмов. Предложенная Клаусом Шнорром схема является модификацией схем Эль-Гамаля (1985) и Фиата-Шамира (1986), но имеет меньший размер подписи. Схема Шнорра лежит в основе стандарта Республики Беларусь СТБ 1176.2-99 и южнокорейских стандартов KCDSA и EC-KCDSA. Она была покрыта патентом США 4999082 (https://www.google.com/patents/US4995082), который истек в феврале 2008 года.

Содержание

Введение

Схемы аутентификации и электронной подписи — одни из наиболее важных и распространенных типов криптографических протоколов, которые обеспечивают целостность информации.

Понять назначение протоколов аутентификации можно легко на следующем примере. Предположим, что у нас есть информационная система, в которой необходимо разграничить доступ к различным данным. Также в данной системе присутствует администратор, который хранит все идентификаторы пользователей с сопоставленным набором прав, с помощью которого происходит разграничение доступа к ресурсам. Одному пользователю может быть одновременно разрешено читать один файл,

изменять второй и в то же время закрыт доступ к третьему. В данном примере под обеспечением целостности информации понимается предотвращение доступа к системе лиц, не являющихся её пользователями, а также предотвращение доступа пользователей к тем ресурсам, на которые у них нет полномочий. Наиболее распространенный метод разграничения доступа, парольная защита, имеет массу недостатков, поэтому перейдем к криптографической постановке задачи.

В протоколе имеются два участника — Алиса, которая хочет подтвердить свой идентификатор, и Боб, который должен проверить это подтверждение. У Алисы имеется два ключа — $\mathbf{K_1}$, открытый (общедоступный), и $\mathbf{K_2}$ — закрытый (приватный) ключ, известный только Алисе. Фактически, Боб должен проверить, что Алиса знает свой закрытый ключ $\mathbf{K_2}$, используя только $\mathbf{K_1}$.

Схема Шнорра — одна из наиболее эффективных среди практических протоколов аутентификации, реализующая данную задачу. Она минимизирует зависимость вычислений, необходимых для создания подписи, от сообщения. В этой схеме основные вычисления могут быть сделаны во время простоя процессора, что позволяет увеличить скорость подписания. Как и DSA, схема Шнорра использует подгруппу порядка q в $\mathbb{Z}_p^*$. Также данный метод использует хеш-функцию $h : \{0,1\}^* \to \mathbb{Z}_p$.

Генерация ключей

Генерация ключей для схемы подписи Шнорра происходит так же, как и генерация ключей для DSA, кроме того, что не существует никаких ограничений по размерам. Заметим также, что модуль p может быть вычислен автономно.

1. Выбирается простое число p, которое по длине обычно равняется 1024 битам.
2. Выбирается другое простое число q таким, чтобы оно было делителем числа $p - 1$. Или другими словами должно выполняться $p - 1 \equiv 0 \pmod{q}$. Размер для числа q принято выбирать равным 160 битам.
3. Выбирается число g, отличное от 1, такое, что $g^q \equiv 1 \pmod{p}$.
4. Пегги выбирает случайное целое число w меньшее q.
5. Пегги вычисляет $y = g^{q-w} \pmod{p}$.
6. Общедоступный ключ Пегги — (p, q, g, y), секретный ключ Пегги — w.

Протокол проверки подлинности

Алгоритм работы протокола

1. *Предварительная обработка*. Алиса выбирает случайное число r, меньшее q, и вычисляет $x = g^r \pmod{p}$. Эти вычисления являются предварительными и могут быть выполнены задолго до появления Боба.
2. *Инициирование.* Алиса посылает x Бобу.
3. Боб выбирает случайное число e из диапазона от 0 до $2^t - 1$ и отправляет его Алисе.
4. Алиса вычисляет $s = r + we \pmod{q}$ и посылает s Бобу.
5. *Подтверждение.* Боб проверяет что $x = g^s y^e \pmod{p}$

Безопасность алгоритма зависит от параметра $\mathbf{t}$. Сложность вскрытия алгоритма примерно равна 2^t. Шнорр советует использовать $\mathbf{t}$ около 72 битов, для $p \geq 2^{512}$ и $q \geq 2^{140}$. Для решения задачи дискретного логарифма, в этом случае, требуется по крайней мере 2^{72} шагов известных алгоритмов.

Пример

Генерация ключей:

- Выбирается простое $p = 48731$ и простое $q = 443$ ($q|p-1$)
- Вычисляется g из условия $g^q = 1 \pmod p$, в данном случае $g = 11444$
- Алиса выбирает секретный ключ $w = 357$ и вычисляет открытый $y = g^{q-w} \pmod p = 7355$ ключ
- Алиса отправляет открытый ключ (p, q, g, y) соответственно равный $(48731, 443, 11444, 7355)$, закрытый оставляет у себя — $w = 357$

Проверка подлинности:

- Алиса выбирает случайное число $r = 274$ и отсылает $x = g^r \pmod p = 37123$ Бобу.
- Боб отсылает Алисе число $e = 129$
- Алиса считает $s = (r + w * e) \pmod q = 255$ и отправляет s Бобу.
- Боб вычисляет $z = g^s * y^e \pmod p = 37123$ и идентифицирует Алису, так как $z = x$.

Атаки на Схему

Пассивный противник

Если в схеме Шнорра предположить, что Алиса является противником, то на шаге 1 она может выбрать x случайным, но эффективным способом. Пусть x — это переданное Алисой число. Предположим, что можно найти два случайных числа e_1 и e_2 такие, что $e_1 \neq e_2$ и для каждого из них Алиса может найти соответствующие s_1 и s_2, для которых подтверждение даст положительный результат. Получаем:

$$x = g^{s_1} y^{e_1} \bmod p$$
$$x = g^{s_2} y^{e_2} \bmod p.$$

Отсюда $g^{s_1} y^{e_1} = g^{s_2} y^{e_2} \pmod p$ или же $y^{e_1 - e_2} = g^{s_2 - s_1} \pmod p$. Так как $e_1 \neq e_2$, то существует $(e_2 - e_1)^{-1} \bmod q$ и, следовательно, $(s_1 - s_2)(e_2 - e_1)^{-1} = w \bmod q$, то есть дискретный логарифм y. Таким образом, либо $e_1, e_2, e_1 \neq e_2$ такие, что Алиса может ответить надлежащим образом на оба из них (при одном и том же x) на шаге 3 протокола, встречаются редко, что означает, что атака Алисы успешна лишь с пренебрежимо малой вероятностью. Либо такие значения попадаются часто, и тогда тот алгоритм, который применяет Алиса, можно использовать для вычисления дискретных логарифмов.

Иными словами, доказано, что в предположении трудности задачи дискретного логарифмирования схема аутентификации Шнорра является стойкой против пассивного противника, то есть корректной.

Активный противник

Активный противник может провести некоторое количество сеансов выполнения протокола в качестве проверяющего с честным доказывающим (или подслушать такие выполнения) и после этого попытаться атаковать схему аутентификации. Для стойкости против активного противника достаточно, чтобы протокол аутентификации был доказательством с нулевым разглашением. Однако свойство нулевого разглашения для схемы Шнорра до сих пор никому доказать не удалось.

Протокол цифровой подписи

Алгоритм Шнорра также можно использовать и в качестве протокола цифровой подписи сообщения M. Пара ключей используется та же самая, но добавляется однонаправленная хеш-функция $H(M)$.

Генерация подписи

1. *Предварительная обработка.* Пегги выбирает случайное число r, меньшее q, и вычисляет $x = g^r \pmod p$. Это стадия предварительных вычислений. Стоит отметить, что для подписи разных сообщений могут использоваться одинаковые открытый и закрытый ключи, в то время как число r выбирается заново для каждого сообщения.
2. Пегги объединяет сообщение M и x и хеширует результат для получения первой подписи:
   $S_1 = H(M|g^r \bmod p)$
3. Пегги вычисляет вторую подпись. Необходимо отметить, что вторая подпись вычисляется по модулю q.
   $S_2 = r + wS_1 \bmod q$.
4. Пегги отправляет Виктору сообщение M и подписи S_1, S_2.

Проверка подписи

1. Виктор вычисляет $X = g^{S_2} y^{S_1} \bmod p$ (либо $X = g^{S_2} y^{-S_1} \bmod p$, если вычислять y как $y = g^w \pmod p$).
2. Виктор проверяет, что $H(M|X) = S_1$. Если это так, то он считает подпись верной.

Эффективность

Основные вычисления для генерации подписи производятся на этапе предварительной обработки и на этапе вычисления $wS_1 \bmod q$, где числа w и S_1 имеют порядок 140 битов, а параметр $r - 72$ бита. Последнее умножение ничтожно мало по сравнению с модульным умножением в схеме RSA.

Проверка подписи состоит в основном из расчета $X = g^{S_2} y^{S_1}$, который может быть сделан в среднем за $1.5l + 0.25t$ вычислений по модулю p, где $l = [log_2 q]$ есть длина q в битах.

Более короткая подпись позволяет сократить количество операций для генерации подписи и верификации: в схеме Шнорра $O(\log_2 q \log_2^2 p)$, а в схеме Эль-Гамаля $O(\log^3 p)$.

Пример

Генерация ключей:

1. $q = 103$ и $p = 2267$. Причем $p = 22q + 1$.
2. Выбирается $f = 2$, который является элементом в поле Z_{2267*}. Тогда $\frac{p-1}{q} = 22$ и $g = 2^{22} \bmod 2267 = 354$
3. Пегги выбирает ключ $w = 30$, тогда $y = 1206$
4. Секретный ключ Пегги — 30, открытый ключ — $(103, 2267, 354, 1206)$.

Подпись сообщения:

1. Пегги нужно подписать сообщение $M = 1000$.
2. Пегги выбирает $r = 11$ и вычисляет {\displaystyle g^{r}=354^{

3. Предположим, что сообщение — {\c , и последовательное соединение означает {\displ . Также предположим, что хеширование этого значения дает дайджест {\displaystyle H(1 . Это означает {\displa ·
4. Пегги вычисляет {\displaystyle S_{2}=r+wS_{1}modq=11+30*200mod103=11+·
5. Пегги отправляет Виктору $M = 1000$, {\displa и {\disp·

Патенты

Схема Шнорра имеет патенты в ряде стран. Например, в США № 4,995,082 от 19 февраля 1991 года (истёк 19 февраля 2008 года). В 1993 году Public Key Partners (PKP) из Саннивейла (Sunnyvale) приобрела мировые права на данный патент. Кроме США, данная схема запатентована также и в нескольких других странах.

Модификации схемы

Модификация схемы, которая была выполнена Эрни Брикеллом (Brickell) и Кевином МакКерли (McCurley) в 1992 году, значительно повысила безопасность данной схемы. В их методе используется число p, которое так же, как и $p-1$, сложно разложить, простой делитель q числа $p-1$ и элемент порядка q в $\mathbb{Z}_p^*$, которые впоследствии применяются в подписи. В отличие от схемы Шнорра подпись в их методе вычисляется уравнением

{\displaystyle s=e\alph·

Преимущества

В то время, как в вычислительном плане модификация Брикелл и МакКерли менее эффективна, чем схема Шнорра, данный метод имеет преимущество, так как основывается на трудности двух сложных задач:

- вычисление логарифма в циклической подгруппе порядка q в $\mathbb{Z}_p^*$;
- разложение $p-1$ на множители.

См. также

- Криптосистема с открытым ключом
- DSA
- Схема Эль-Гамаля

Примечания

Литература

- *Schnorr C.P.* Efficient Signature Generation by Smart Cards. — J. Cryptology, 1991. — С. 161—174.
- *Schnorr C.P.* Efficient Identification and Signatures for Smart Cards.Advances in Cryptology - CRYPTO'89. Lecture Notes in Computer Science 435. — 1990. — С. 239 — 252.
- *A. Menezes, P.van Oorschot, S. Vanstone.* Handbook of Applied Cryptography. — CRC Press, 1996. — 816 с. — ISBN 0-8493-8523-7.

- *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.
- *Варновский Н. П.* Криптографические протоколы (http://nature.web.ru/db/msg.html?mid=1157083&uri=node18.html) // Введение в криптографию (http://nature.web.ru/db/msg.html?mid=1157083&uri=book.html) / Под редакцией В. В. Ященко. — Питер, 2001. — 288 с. — ISBN 5-318-00443-1. — [Архивировано (https://web.archive.org/web/20080225102710/http://nature.web.ru/db/msg.html?mid=1157083&uri=book.html) 25 февраля 2008 года.]

Ссылки

- RFC 8235

В статье есть список источников, но **не хватает сносок**.
Без сносок сложно определить, из какого источника взято каждое отдельное утверждение. Вы можете улучшить статью, проставив сноски на источники, подтверждающие информацию. Сведения без сносок могут быть удалены. *(3 января 2015)*

Источник — https://ru.wikipedia.org/w/index.php?title=Схема_Шнорра&oldid=148647110

Эта страница в последний раз была отредактирована 19 сентября 2025 года в 14:52.

Текст доступен по лицензии Creative Commons «С указанием авторства — С сохранением условий» (CC BY-SA); в отдельных случаях могут действовать дополнительные условия.
Wikipedia® — зарегистрированный товарный знак некоммерческой организации «Фонд Викимедиа» (Wikimedia Foundation, Inc.)