Протокол Фиата — Шамира

Материал из Википедии — свободной энциклопедии

Протокол Фиата — Шамира — это один из наиболее известных протоколов идентификации с нулевым разглашением (Zero-knowledge protocol). Протокол был предложен Амосом Фиатом (англ. *Amos Fiat*) и Ади Шамиром (англ. *Adi Shamir*)

Пусть **A** знает некоторый секрет **s**. Необходимо доказать знание этого секрета некоторой стороне **B** без разглашения какой-либо секретной информации. Стойкость протокола основывается на сложности извлечения квадратного корня по модулю достаточно большого составного числа **n**, факторизация которого неизвестна.

Содержание

Описание протокола

A доказывает **B** знание **s** в течение **t** раундов. Раунд называют также аккредитацией. Каждая аккредитация состоит из 3х этапов.

Предварительные действия

- Доверенный центр **T** выбирает и публикует модуль $n = p * q$, где **p**, **q** — простые и держатся в секрете.
- Каждый претендент **A** выбирает **s** взаимно-простое с **n**, где $s \in [1, n-1]$. Затем вычисляется **V** $= s^2 \pmod n$. **V** регистрируется **T** в качестве открытого ключа **A**

Передаваемые сообщения (этапы каждой аккредитации)

- A⇒B : $x = r^2 \pmod n$
- A⇐B : $e \in 0, 1$
- A⇒B : $y = r * s^e \pmod n$

Основные действия

Следующие действия последовательно и независимо выполняются **t** раз. **B** считает знание доказанным, если все **t** раундов прошли успешно.

- **A** выбирает случайное **r** , такое, что $r \in [1, n-1]$ и отсылает $x = r^2 \pmod n$ стороне **B** (доказательство)
- **B** случайно выбирает бит **e** (**e**=0 или **e**=1) и отсылает его **A** (вызов)
- **A** вычисляет **y** и отправляет его обратно к **B**. Если **e**=0, то $y = r$, иначе $y = r * s \pmod n$ (ответ)
- Если **y**=0, то **B** отвергает доказательство или, другими словами, **A** не удалось доказать знание **s**. В противном случае, сторона **B** проверяет, действительно ли $y^2 = x * v^e \pmod n$ и, если это так, то происходит переход к следующему раунду протокола.

Выбор **e** из множества {0,1} предполагает, что если сторона **A** действительно знает секрет, то она всегда сможет правильно ответить, вне зависимости от выбранного **e**. Допустим, что **A** хочет обмануть **B**. В этом случае **A**, может отреагировать только на конкретное значение **e**. Например, если **A** знает, что получит **e**=0, то **A** следует действовать строго по инструкции и **B** примет ответ. В случае, если **A** знает, что получит **e**=1, то **A** выбирает случайное **r** и отсылает $x = r^2/v$ на сторону **B**, в результате получаем нам нужное $y = r$. Проблема заключается в том, что **A** изначально не знает какое **e** он получит и поэтому не может со 100 % вероятностью выслать на сторону **B** нужные для обмана **r** и **x** ($x = r^2$ при **e**=0 и $x = r^2/v$ при **e**=1). Поэтому вероятность обмана в одном раунде составляет 50 %. Чтобы снизить вероятность жульничества (она равна $1/2^t$)) **t** выбирают достаточно большим (**t**=20, **t**=40). Таким образом, **B** удостоверяется в знании **A** тогда и только тогда, когда все **t** раундов прошли успешно.

Пример

- Пусть доверенный центр выбрал простые **p**=683 и **q**=811, тогда **n**=683*811=553913. **A** выбирает **s**=43215.

Откуда $v = 43215^2 \pmod{553913} = 1867536225 \pmod{553913} = 295502$

- **A** выбирает **r**=38177 и считает
  $x = 38177^2 \pmod{553913} = 1457483329 \pmod{553913} = 138226$
- Если **B** отправил **e**=0, то **A** возвращает y=38177. Иначе, **A** возвращает
  $y = 38177 * 43215 \pmod{553913} = 1649819055 \pmod{553913} = 266141$
- Проверка **B**: $y^2 \equiv x * v^e \pmod n$

Если **e** было равно 0, то $y^2 = 38177^2 \pmod{553913} = 1457483329 = 138266$ Подтверждено.

Иначе, $y^2 = 266141^2 \pmod{553913} = 70831031881 \pmod{553913} = 514832$

и $x * v = 138226 * 295502 \pmod{553913} = 40846059452 \pmod{553913} = 514832$ Подтверждено.

Литература

- *Menezes A., van Oorschot P., Vanstone S.* 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.

Источник — https://ru.wikipedia.org/w/index.php?title=Протокол_Фиата_—_Шамира&oldid=143702268

Эта страница в последний раз была отредактирована 27 февраля 2025 года в 15:10.

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.)