Протоколы с нулевым разглашением и их применения.

Zero-knowledge protocols and their applications.

Эссе по курсу "Защита информации", кафедра радиотехники.

Андрей Уланов
гр. 112, ФРТК, МФТИ.

21 мая 2005 г.

Содержание

1 Введение

"Волк подслушал, как поет коза. Вот раз коза ушла, волк побежал к избушке и закричал толстым голосом:

- Вы, детушки! Вы, козлятушки! Отопритеся, отворитеся!

Козлята ему отвечают:

- Слышим, слышим - да не матушкин это голосок! Наша матушка поет тонюсеньким голосом и не так причитает.

Волку делать нечего. Пошел он в кузницу и велел себе горло перековать, чтоб петь тонюсеньким голосом. Только ушла коза, волк опять шасть к избушке, постучался и начал причитывать тонюсеньким голосом:

- Козлятушки, ребятушки! Отопритеся, отворитеся!

Козлята отворили дверь, волк кинулся в избу и всех козлят съел..."

«Волк и семеро козлят», русская народная сказка.

Во многих криптографических системах возникает задача одной стороне A (*доказывающая сторона*) доказать знание секрета другой стороне B (*проверяющая сторона*), причем сделать это необходимо таким образом чтобы сторона B после этого не знала сам секрет. То есть A демонстрирует знание какой-то информации без разглашая какой-либо части этой информации. Впервые понятие протоколов с нулевым разглашением было введено в работе Гольдвассера, Микали и Ракоффа в 1985 г.[1]. Такие протоколы позволяют решить проблемы которыми обладают все методы авторизации по паролю: (1) необходимость хранить пароль на сервере либо (2) простота отслеживания пароля третьей стороной, подслушивающей процесс авторизации.

Как правило все протоколы с нулевым разглашением носят вероятностный характер. Это означает что проверяющая сторона никогда не может быть полостью уверена в знании стороной A секрета, но может убедиться в этом с точностью до любой, наперед заданной, вероятностью за конечное время.

Итак *протоколом доказательства с нулевым разглашением* называется протокол доказательства, обладающий следующими свойствами[1]:

Полнота. То есть доказывающий всегда сможет доказать знание секрета если он им действительно обладает.

Корректность. То есть доказывающий не может продемонстрировать знание секрета если он в действительности не владеет таким знанием.

Свойство нулевого разглашения. Данное свойство означает что любую информацию которую получает проверяющая сторона (либо третья подслушивающая сторона) она смогла бы также получить самостоятельно каким-то полиномиальным алгоритмом вообще без взаимодействия с A.

Необходимо заметить что многие протоколы призванные обеспечивать аутентификацию пользователя проверяя знание им пароля (или секретного ключа в системах с открытым ключом) не передавая в открытом виде сам пароль (или закрытый ключ) не являются с математическом точки зрения алгоритмами с абсолютно нулевым разглашением по той причине что не удовлетворяют последнему свойству. Такие алгоритмы называют иногда *доказательством с вычислительно нулевым разглашением.*

2 Протоколы с нулевым разглашением

2.1 Простейший пример: пещера Али Бабы (Ali Baba)

Классическим примером протокола доказательства с нулевым разглашением является протокол доказательства знания пароля к двери внутри круговой пещеры. Пусть Алиса (Alice) знает этот пароль и хочет доказать его знание Бобу (Bob) без разглашения самого пароля. Используется следующий протокол:

[1]Здесь автор умышленно избегает точного математического определения по той причине что это не имеет смысла в контексте данной статьи носящей вводный характер. Для более полного теоретического изложения см., например, [2].

1. Алиса заходит в пещеру и подходит к двери с произвольной стороны так чтобы Боб не знал с какой стороны находится Алиса.

2. Боб заходит в пещеру и просит выйти Алису с какой либо из сторон пещеры (слева или справа).

3. Алиса зная пароль к двери всегда сможет выполнить пожелание Боба, появившись с любой стороны.

После каждой итерации уверенность Боба в том что Алиса знает секрет увеличивается вдвое. Таким образом после k успешно выполненных операций вероятность того что Алиса на самом деле обманывает Боба равна $1/2^k$.

2.2 Другой простейший пример: Кубик Рубика (Rubic's Cube)

Следующий пример так же как и предыдущий носит чисто гипотетический характер. Пусть Алиса знает как решить Кубик Рубика из какой-то позиции (назовем ее *исходной*) и хочет доказать это Бобу, при этом она не хочет чтобы Боб также научился складывать кубик из данной позиции. Для решения этой задачи может использоваться протокол состоящий из нескольких последовательных выполнений следующих действий:

1. Алиса выбирает произвольную другую позицию кубика и показывает ее Бобу.

2. Боб просит сделать одно из следующих действий:

   (a) показать как из выбранной позиция собрать исходную либо

   (b) показать как решить выбранную позицию.

3. Алиса выполняет просьбу Боба.

Очевидно Алиса всегда сможет доказать Бобу умение решать исходную позицию если она действительно таким умением обладает. В противном же случае она не всегда сможет выполнить последний пункт. Так же любое количество итераций никаким образом не поможет Бобу выяснить как решается исходная позиция.

2.3 Протокол на основе задачи об изоморфизме графов

Пусть дана пара графов $G_1 = (U, E_1)$ и $G_2 = (U, E_2)$, здесь U – множество вершин графа, а E_1 и E_2 – множества ребер. Графы G_1 и G_2 называют изоморфными если существует перестановка φ вершин графа которая переводит один граф в другой. Задача нахождения такой перестановки и поиск ответа на вопрос о её существовании есть сложная математическая задача не решаемая за полиномиальное время.

Итак рассмотрим следующий протокол. Пусть φ – изоморфизм графов G_1 и G_2 знанием которого обладает Алиса. Она доказывает это знание Бобу:

1. Алиса выбирает случайную перестановку π на множестве U и передает граф πG_1 Бобу.

2. Боб выбирает случайный бит α и пересылает его Алисе.

3. Если $\alpha = 1$, то Боб пересылает Алисе перестановку π, иначе перестановку $\pi \circ \varphi$.

4. При $\alpha = 0$ Боб проверяет является ли полученная перестановка изоморфизмом между G_2 и H, либо G_1 и H при $\alpha = 0$.

Данный протокол интересен только с теоретической точки зрения. Применение его на практике невозможно по причине необходимости передавать огромное количество данных.

2.4 Протокол Фейга-Фиата-Шамира (Feige-Fiat-Shamir)

Следующий протокол основывается на сложности вычисления квадратного корня числа по модулю большого числа с неизвестным разложением на простые множители.

В протоколе предполагает что обе стороны заранее снабжены каким-то числом $n = pq$. При этом разложение n на простые множители считается неизвестным для всех участников протокола. Доказывающая сторона (Алиса) выбирает секретное число s, взаимно простое с n, далее вычисляет значение $v = s^2 \bmod n$ и публикует значение v объявляя его своим открытым ключом.

Как и все предыдущие, протокол Фейга-Фиата-Шамира состоит в последовательном выполнении следующих итераций:

1. Алиса выбирает число z: $1 < z < n - 1$.

2. Алиса вычисляет и посылает проверяющей стороне (Бобу) число $x = z^2 \bmod n$.

3. Боб выбирает случайный бит α и пересылает его Алисе.

4. Алиса пересылает Бобу число y:

$$y = \begin{cases} z, & \text{если } \alpha = 0 \\ zs \bmod n, & \text{если } \alpha = 1 \end{cases}$$

5. Боб проверяет что $y \neq 0$ и $y^2 \equiv xv^\alpha \pmod{n}$.

Рассмотрим последнюю проверку. Если $\alpha = 0$, то $y = z$, $y^2 = z^2$, $xv^\alpha = x$, и проверка означает проверку на эквивалентность z^2 и x по модулю n, что должно следовать из первого пункта протокола. Если $\alpha = 1$, то $y = zs \bmod n$, $y^2 = z^2 s^2 \bmod n$, $xv^\alpha = xv = xs^2 \pmod{n}$. И проверка означает проверку на эквивалентность по модулю n чисел $z^2 s^2$ и xs^2, что опять же должно вытекать из первого пункта.

3 Протоколы с нулевым разглашением на практике

Как было отмечено выше многие другие криптографические протоколы идентификации не являются в точном математическом смысле протоколами с абсолютно нулевым разглашением. Однако совсем не этот фактор имеет в данном случает решающее значение.

Многие протоколы в том числе протоколы на основе систем с открытым ключом требуют огромного количества вычислений с обоих сторон. В то же время они обладают тем существенным преимуществом что для полной проверки доказываемого знания достаточно одной итерации. В случае же с протоколами с нулевым разглашением вычисления как правило более просты. Но в тоже время они требуют большого количества итераций прежде чем проверяющая сторона сможет убедиться в идентичности доказывающей стороны с достаточной степенью вероятности.

Описанные свойства и определили в основном возможные применения протоколов с нулевым разглашением. Очевидно в силу требования к большому количеству итераций их применение в компьютерных сетях связано с трудностями. С другой стороны использование протоколов со сложными вычислениями невозможно на сравнительно простых устройствах с малым количеством памяти таких как смарт-карты. Последние и приводятся чаще всего в качестве основного примера где возможно использование протоколов с нулевым разглашением.

Список литературы

[1] *Goldwasser S., Micali S., Rackoff C.* The knowledge complexity of interactive proof systems // SIAM J. Comput. V. 18, No 1, 1989. P. 186-208.

[2] Введение в криптографию. *Под редакцией В.В.Ященко.* МЦНМО 2000.

[3] *Hannu A. Aronsson.* Zero Knowledge Protocols and Small Systems[2]. Department of Computer Science, Helsinki University of Technology.

[4] *А.П.Алферов, А.Ю.Зубов, А.С.Кузьмин, А.В.Черемушкин.* Основы криптографии. Москва, Гелиос АРВ, 2002.

[2] http://www.tml.hut.fi/Opinnot/Tik-110.501/1995/zeroknowledge