Индивидуальный проект
Геометрическая криптография

Арсений Балобанов

5 января 2015 г.

Введение

Геометрическая криптография - отдельная область криптографии, впервые предложенная к изучению Ади Шамиром, Рональдом Линн Ривестом и Майком Бурместером в 1996 году [1]. В геометрической криптографии в качестве сообщений и шифров выступают такие геометрические объекты как угол и интервал, а вычисления производятся с помощью циркуля и линейки. В основу протоколов геометрической криптографии ложатся неразрешимые или трудноразрешимые задачи геометрии, например, удвоение куба, квадратура круга. Методы геометрической криптографии мало применимы на практике, однако, они расширяют аудиторию науки в целом и могут быть использованы в педагогике в качестве поясняющих примеров более сложных криптографических протоколов.

Геометрическая криптография

Современная теория алгоритмов основывается на представлении данных в виде последовательностей символов (обычно битов), и осуществлению над ними операций из довольно небольшого набора (например, конъюнкция и дизъюнкция). Но вычисления можно производить и над другими представлениями данных. Например, довольно хорошо изучена модель построения циркулем и линейкой. Напомним стандартные операции, разрешенные в построении:

1. Через две различные точки можно провести единственную прямую
2. Можно построить точку пересечения двух различных пересекающихся прямых
3. Имея две различные точки A и B можно построить три точки C_1, C_2, C_3 отличные от A и B такие что:
   (a) C_1 лежит на прямой проходящей через A и B между A и B
   (b) C_2 лежит на прямой проходящей через A и B, и B между A и C_2
   (c) C_3 не лежит на прямой проходящей через A и B
4. Для интервала AB и луча CD можно построить точку E на луче CD такую, что AB и CE конгруэнтны
5. Можно построить точку (точки) пересечения окружности и пересекающей ее прямой

Подробнее об аксиомах и аксиоматических понятиях, таких как “точка”, “прямая”, “конгуэнтность” можно прочитать в [2].

Неотъемлемой частью криптографических протоколов является возможность создания “секретов”, скрытых от противника. Они не могут быть построены циркулем и линейкой с помощью имеющихся объектов, иначе, противник сможет найти их. Поэтому вводится дополнительная аксиома выбора случайных точек:

6. На единичной окружности можно построить случайную точку

Протокол идентификации

Алиса (Прувер) хочет установить способ доказательства описания своей личности Бобу (Верификатору).

Инициализация

Алиса строит случайный угол X_A с помощью аксиомы 6. Затем строит угол Y_A равный утроенному углу X_A, после построения публикует копию угла Y_A. Задача утроения угла подвластна любому школьнику знакомому с геометрией, а вот задача деления угла на три равных, наоборот, не разрешима. Трисекция угла выступает своего рода односторонней функцией в геометрической криптографии, поэтому Алиса уверена, что только она знает величину угла X_A.

Протокол

1. Алиса передает Бобу копию угла R, который она построила утроением угла K, который она построила случайным образом

2. Боб подкидывает монетку и сообщает Алисе результат

3. Если Боб говорит "орел", Алиса передает Бобу копию угла K и Боб проверяет, что $3 \cdot K = R$
   Если Боб говорит "решка", Алиса передает Бобу копию угла $L = K + X_A$, и Боб проверяет, что $3 \cdot L = R + Y_A$

Эти три шага повторяются независимо t раз, и Боб принимает доказательство Алисы только если все t проверок успешны.

Утверждение 1
Описанный выше протокол является протоколом доказательства знания угла X_A (личности Алисы), с ошибкой 2^{-t}, а также протоколом с нулевым разглашением.

Доказательство.
Если Алиса и Боб будут следовать протоколу, то, ясно что, Боб примет доказательство Алисы.
Самозванец же, который не знает угол X_A, не сможет построить оба угла L и K, иначе он смог бы построить угол $L - K = X_A$. Поэтому, Боб примет доказательство Алисы с вероятностью не более чем $\frac{1}{2}$ на каждой итерации,

и следовательно, с вероятностью не более 2^{-t} на всех t итерациях. Отсюда следует, что данный протокол - протокол доказательства знания (Proof of knowledge) X_A [3].
Для доказательства нулевого разглашения, будем симулировать то, что "видит" Боб во время исполнения протокола. Боб "видит" сообщения Алисы и свои броски монеты. Эти состояния можно записать как тройки (R, "орел", K) и (R, "решка", L). Для симуляции владельца секрета, можно выбрать K случайно, и взять $R = 3 \cdot K$, выбрать случайное L и разрешить $3 \cdot L = R + Y_A$ относительно R. Таким образом, Боб может симулировать действия Алисы, тем самым получает нулевое разглашения относительно X_A. ■

Теорема 1 *(Гаусса - Ванцеля)*
Правильный n-угольник можно построить с помощью циркуля и линейки тогда и только тогда, когда $n = 2^k \cdot p_1 \cdot \ldots \cdot p_m$, где p_i - различные простые числа Ферма ($2^{2^a} + 1$).

Теорема 2 *(Ванцель)*
Задача трисекции угла α разрешима тогда и только тогда, когда разрешимо в квадратных радикалах уравнение

$$4x^3 - 3x - cos(\alpha) = 0$$

Применения протокола идентификации

Геометрическая криптография может адаптировать многие криптографические примитивы. Рассмотрим два расширения описанного протокола: параллельное исполнение и "множественный секрет".

Для параллельного исполнения t итераций протокола выполняются одновременно:

- Алиса посылает Бобу t копий углов R_i
- Боб подбрасывает t монет
- Алиса посылает Бобу копии соответствующих углов (шаг 3)

Ожидаемое число испытаний в этом случае - 2^t. Этот протокол может быть реализован, так как не накладывается никаких сложностных ограничений на построения.

Замечание 1
Протокол параллельной идентификации также будет являться протоколом с нулевым разглашением, в отличие от традиционной криптографии, в которой не известно будет ли параллельное исполнения протокола с нулевым разглашением протоколом с нулевым разглашением.

Для множественного секрета Алиса строит k случайных углов $X_{A_1}, \ldots, X_{A_k}$ и публикует их утроения $Y_{A_1}, \ldots, Y_{A_k}$. Затем Алиса доказывает Бобу, что она знает все углы $X_{A_1}, \ldots, X_{A_k}$ с помощью следующего протокола, повторенного t раз:

1. Алиса посылает Бобу копию угла R, построенного утроением случайного угла K
2. Боб посылает Алисе строку битов $b_1, \ldots, b_k$ - результат подбрасывания k монет
3. Алиса посылает Бобу копию угла $L = K + \sum_{i=1}^{i=k} b_i X_{A_i}$ и Боб проверяет, что $3 \cdot L = R + \sum_{i=1}^{i=k} b_i Y_{A_i}$

Боб принимает доказательство Алисы только в случае принятия на всех t итерациях. Легко видеть, что ошибка для этого протокола уже 2^{-kt}.

Протокол аутентификации

Пусть m - целое число, которое Алиса хочет подтвердить. Это ограничение не сильное в виду того, что Алиса может опирать только на геометрические объекты, которые можно построить циркулем и линейкой, коих счетно.

В протоколе Алиса строит два угла X_{A_1} и X_{A_2}, и публикует их утроения Y_{A_1} и Y_{A_2}. Алиса доказывает Бобу, что она знает угол $Z = m \cdot X_{A_1} + X_{A_2}$ использую протокол идентификации, рассмотренный выше:

1. Алиса посылает Бобу копию угла R, построенного утроением случайного угла K
2. Боб подбрасывает монетку, и сообщает Алисе бит b
3. Алиса посылает Бобу угол $L = K + b(m \cdot X_{A_1} + X_{A_2})$
   Боб проверяет, что $3 \cdot L = R + b(m \cdot Y_{A_1} + Y_{A_2})$

Обобщение протокола идентификации

Пусть N - дополнительный угол, используемый как модуль при выполнении построений суммы и разности углов. Пусть Y - угол, который нужно разделить на три по модулю N. Тогда у уравнения $Y = 3 \cdot X \ mod(N)$ имеется три решения, которые отличаются на множители $\frac{N}{3}$. Поэтому каждый, кто знает два решения X_1 и X_2 может осуществлять трисекцию по модулю N. Подобное свойство позволяет обобщать многие криптографические конструкции, использующие теорию чисел, в которых знание двух различных корней числа y по модулю n позволяет факторизовать n. Рассмотрим одно применение.

Предположим, что распределение точек в аксиоме 6 не равномерное, тогда описанный протокол идентификации уже не будет протоколом с нулевым разглашением, потому что уже нельзя будет симулировать (R, "решка", L) выбирая случайное L и решая $3 \cdot L = R + Y_A$ (так как R может иметь другое распределение). Поэтому Боб может получить некоторую информацию и построить "секретный" угол Алисы - X_A. Покажем, как использовать соображения выше для усиления безопасности протокола в этом случае.
Во-первых, распределение углов должно быть непрерывным, в частности, вероятность выбора конкретного угла K должна быть ноль. Иначе Боб сможет построить углы K и $L = K + X_A$, а из них построить X_A. Пусть N - угол, который не может разделить на три части ни Алиса, ни Боб (например, N выбирается случайно доверенным лицом). Для защиты Алиса будет сообщать Бобу не абсолютные значения углов, а их значения по модулю N. Подобный шаг не сделает распределение углов равномерным, но сделает абсолютно не понятным для Боба какая именно из трех трисекций угла Y_A: X_A, $X_A + \frac{N}{3}$, $X_A + 2\frac{N}{3}$ используется Алисой в L. Даже если Боб будет иметь три такие возможности, он выберет правильную с вероятностью не более $\frac{1}{3}$. Если предположить, что эту схему можно взломать и Боб может построить трисекцию Y_A, с вероятностью $\frac{2}{3}$ это будет не та трисекция, использованная Алисой, поэтому подобное построение с некоторой фиксированной вероятностью приведет к построению трисекции угла N.

Литература

[1] Mike Burmester, Ronald L Rivest and Adi Shamir *"Geometric Cryptography Identification by Angle Trisection"* e-Prints, US Department of Energy, OSTI. Retrieved 19 June 2014.

[2] *The New Encyclopedia Brittanica*, Volume 19, Geometry, pages 887–936, 1995.

[3] S. Goldwasser, S. Micali and C. Rackoff. *"The Knowledge Complexity of Interactive Proof Systems"* Siam J. Comput., Vol 18 (1), pages 186–208, 1989.