МЕТОД ШНОРРА В КРИПТОГРАФИИ

Лапытько А. И., Свиридчик В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Стройникова Е. Д. – ст. преп. кафедры информатики

Данная работа посвящена одному из наиболее эффективных методов аутентификации, а именно методу Шнорра. Для его реализации были разработаны две программы на языках программирования Python (в среде PyCharm) и C++ (в среде Qt). Проведено сравнение метода Шнорра с другими методами аутентификации, изучены сферы их применения.

В наше время, когда цифровые технологии внедряются во все сферы человеческой жизни, людям приходится адаптироваться: переносить личные данные, важную информацию на вычислительные устройства. И вполне естественно скрывать некоторую информацию от отдельных лиц. Для этого в цифровом пространстве используются методы, или схемы, аутентификации. Схема Шнорра была представлена немецким математиком Клаусом Шнорром как видоизменение схем Эль-Гамаля и Фиата – Шамира. Основным преимуществом метода Шнорра является меньший размер подписи. После публикации автор метода оформил множество патентов.

Во время разработки биткоина Сатоше Накамото было необходимо выбрать метод реализации цифровой подписи. Первоначально был выбран ECDSA, однако в 2014 г. начал внедряться метод Шнорра.

Большинство алгоритмов криптографии с открытым ключом основывается на таких задачах, как разложение на множители (он же метод факторизации, основанный на сложности разложения на множители большого числа), а также решение дискретного логарифма. Безопасность данного способа шифрования основывается на том, что вычислить $a^x \pmod p$ легко, например быстрым (бинарным) возведением в степень, а вот вычислить соответствующий логарифм довольно трудно. Наиболее популярными алгоритмами, использующими в своей основе проблему дискретного логарифма в конечном поле, являются:

1. Elgamal (схема Эль-Гамаля, 1985 г.) – усовершенствованная версия алгоритма Диффи – Хеллмана, вошедшая в основу большинства последующих схем шифрования.
2. Схема Шнорра (1991 г.) – модификация схем Эль-Гамаля и Фиата – Шамира.
3. DSA (Digital Signature Algorithm, 1998 г.), но только для электронной подписи. Так же, как и схема Шнорра, является модификацией схемы Эль-Гамаля.
4. ECDSA (Elliptic Curve Digital Signature Algorithm, 1999 г.) – модификация схемы DSA, но основанная на эллиптических кривых. Тем не менее, для криптовалюты схема Шнорра всё ещё является приоритетной.
5. BLS (Боне, Линна, Шахама) – альтернатива подписи Шнорра в криптовалюте.

Для демонстрации схемы Шнорра авторами данной работы были разработаны две программы на языках программирования Python (в среде PyCharm) и C++ (в среде Qt), алгоритм и результат работы которой представлен на рисунке 1.

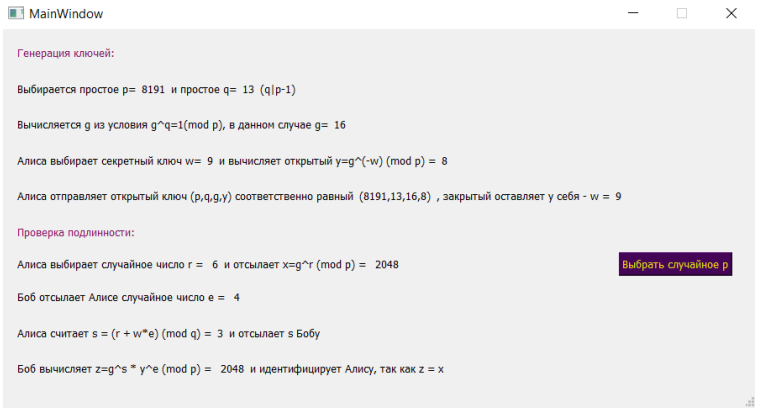

Рисунок 1 – Алгоритм и результат работы программы на языке C++

Разработанные программы доступны по ссылкам:
1) https://github.com/AHTOH2001/MGiA;
2) https://github.com/sviridchik/shnor/tree/master/sign.

Алгоритм ECDSA неплох, он выполняет поставленную перед ним задачу, но не более того. К

примеру, нельзя с помощью ECDSA комбинировать ключи и подписи и нельзя одновременно подтвердить каждую подпись, что особенно полезно в транзакциях с мультиподписью.

Алгоритм Шнорра в этом плане более эффективен: он способен скомбинировать набор подписей и ключей в один блок и даёт возможность их проверить гораздо быстрее, чем каждый ключ и подпись в отдельности. Но и он имеет некоторые недостатки, такие как:

- создание нескольких подписей для каждого блока;
- неудобство продолжительного хранения блока, т. к. используются несколько коммуникационных каналов для подписи;
- многократное генерирование случайного числа при комбинировании вместо того, чтобы выбрать одну случайную точку, как в ECDSA;
- использование пары простых чисел.

Алгоритм BLS способен решить все вышеперечисленные проблемы:

- используется одно простое число для подписи;
- генератор случайных чисел вообще не используется;
- блок можно представить одной подписью;
- нет необходимости в нескольких канал для подписи.

Это результат того, что в алгоритмах ECDSA и Шнорра хешируется сообщение и используется этот же хеш, представляющий собой число, в подписи. А в алгоритме BLS сразу получается хеш, представляющий собой эллиптическую кривую, такую же, как и те, которые используются в криптовалюте. Таким образом, несмотря на все преимущества подписи BLS он может использоваться только в криптовалюте, т. е. он не так гибок, как алгоритм подписи Шнорра.

Схема Шнорра лежит в основе стандарта Республики Беларусь СТБ 1176.2-99 и южнокорейских стандартов KCDSA и EC-KCDSA.

Список использованных источников:

1. Стройникова, Е. Д. Основы прикладной алгебры : учеб.-метод. пособие / Е. Д. Стройникова. – Минск : БГУИР, 2010. – 120 с.

2. Википедия, схема Шнорра [Электронный ресурс]. – Режим доступа : https://ru.m.wikipedia.org/wiki/Схема_Шнорра.

3. Лекция 3: Цифровая подпись [Электронный ресурс]. – Режим доступа : https://www.intuit.ru/studies/courses/553/409/lecture/9379?page=5.

4. Лекция 3: Цифровая подпись, страница 5 [Электронный ресурс]. – Режим доступа : https://www.intuit.ru/studies/curriculums/15720/courses/409/lecture/9379?page=5.

5. Глава 21 Схемы идентификации [Электронный ресурс]. – Режим доступа : https://studfile.net/preview/1826159/page:38/.

6. Схемы идентификации 21.1 FEIGE-FIAT-SHAMIR [Электронный ресурс]. – Режим доступа : http://wclipart.narod.ru/doc-1/kind-crip23-1-pag.html.