СХЕМА ШНОРРА В КРИПТОГРАФИИ

Колесников П. В., Антихович М. В., Малец В. С.

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

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

Данная работа посвящена одному из наиболее эффективных способов проверки подлинности, а именно способу Шнорра. Схема Шнорра дает возможность проверить подпись сообщения и убедиться в подлинности отправителя. Она также обладает свойствами неделимости, невозможности отказаться от подписи и защиты от повторной передачи сообщения. Проведено раскрытие сути протокола Шнорра, сравнение способа Шнорра с другими методами аутентификации, изучение применения данной схемы в сфере информационной безопасности.

Протокол цифровой подписи Шнорра был разработан криптографом Клаусом Шнорром в 1989 году и является одним из наиболее распространенных протоколов данного типа. Эта схема, являющаяся улучшенной версией схемы Эль-Гамаля, используется для обеспечения аутентификации сообщений и цифровых подписей. Цифровые подписи представляют собой математические схемы, которые используются для проверки подлинности и целостности цифровых сообщений. Они позволяют доказать, что сообщение было отправлено конкретным отправителем (подлинность) и не было изменено в процессе передачи (целостность).

В отличие от физической подписи, где отправитель аутентифицирует себя с помощью своего уникального почерка с определенным намерением, цифровая подпись использует математические алгоритмы. Схема Шнорра является одной из самых простых, эффективных и создает короткие подписи. Она также используется для реализации "Proof Of Knowledge", интерактивного доказательства, в котором проверяющий "убеждает" проверяемого в том, что он знает нечто "X".
В случае с доказательством подписи, это означает, что верификатор должен быть убежден в том, что он общается с пользователем, который знает закрытый ключ, соответствующий открытому ключу.

Пара закрытый-открытый ключ (или асимметричный ключ) - это метод криптографии, где для шифрования и расшифровки информации используются два разных ключа: открытый и закрытый.

Открытый ключ (public key) – это криптографический ключ, который может быть раскрыт всем. Этот ключ используется для шифрования сообщений и файлов, которые будут отправлены конкретному получателю. Получатель использует свой закрытый ключ, чтобы расшифровать сообщение, таким образом, только получатель может прочитать сообщение, даже если кто-то перехватывает сообщение в процессе передачи.

Закрытый ключ (private key) – это секретный ключ, который используется для расшифровки сообщений, зашифрованных открытым ключом. Закрытый ключ не должен быть раскрыт никому, за исключением владельца. Владелец использует закрытый ключ для расшифровки сообщений, которые были зашифрованы его открытым ключом.

Таким образом, открытый ключ может быть свободно распространен и использован для шифрования данных, но не может быть использован для расшифровки. Закрытый ключ, с другой стороны, известен только владельцу ключа и используется для расшифровки данных, зашифрованных с помощью открытого ключа.

Пары закрытый-открытый ключ являются основой большинства криптографической безопасности, от безопасного просмотра веб-страниц до банковских операций и криптовалют. Пары закрытый-открытый ключ являются асимметричными, то есть по одному ключу можно вычислить другой, но не наоборот. Это позволяет кому-то делиться открытым ключом публично, но быть уверенным, что никто не сможет вычислить закрытый ключ (который хранится в тайне и безопасности).

Пары асимметричных ключей используются в двух основных приложениях:

- Аутентификация, где вы доказываете, что знаете закрытый ключ.
- Шифрования, где сообщения могут быть закодированы, и только человек, обладающий закрытым ключом, может расшифровать и прочитать сообщение.

Безопасность схемы Шнорра основана на неразрешимости некоторых проблем с дискретным логарифмом. Она использует криптографические хеш-функции для генерации уникальных идентификаторов сообщений, что позволяет обеспечить целостность данных и защитить их от подделки. Хеш-функция принимает на вход сообщение произвольной длины и возвращает фиксированный хеш-код конкретной длины. В качестве примера рассмотрим процесс создания цифровой подписи. Для создания цифровой подписи отправитель должен выполнить следующие шаги:

1. Выбрать простое число p и генератор g, такие, что g является первообразным корнем по модулю p.

2. Выбрать случайное число k из интервала [1, p-1].
3. Вычислить R = g^k (mod p).
4. Вычислить хеш-значение h от сообщения m.
5. Вычислить e = h(R||m), где || означает конкатенацию R и m.
6. Вычислить s = k - x*e (mod (p-1)), где x – это секретный ключ отправителя.
7. Цифровая подпись будет представлена парой (R, s).

Для проверки подписи получатель должен выполнить следующие шаги:

1. Вычислить хеш-значение h от сообщения m.

Получатель должен использовать ту же хеш-функцию, которую использовал отправитель при создании подписи. Хеш-значение h является уникальным идентификатором сообщения и используется для проверки подписи.

2. Вычислить v = g^s * y^e (mod p), где y – это открытый ключ отправителя.

Получатель должен использовать открытый ключ отправителя, чтобы вычислить значение v. Значение v – это результат комбинации двух частей цифровой подписи: R и s. Часть R была выбрана отправителем на этапе создания подписи, а часть s была вычислена отправителем при помощи его секретного ключа. Получатель вычисляет v с помощью открытого ключа отправителя, которым он располагает, и значений R и s, которые были включены в подпись.

3. Если R = v, то подпись считается действительной.

Получатель сравнивает значение R из подписи с вычисленным значением v. Если они равны, то подпись считается действительной, и получатель может быть уверен, что сообщение не было изменено и что оно было отправлено именно тем отправителем, чья цифровая подпись была получена.

Чтобы наглядно продемонстрировать схему Шнорра, авторы разработали консольное приложение на языке программирования C++ (в Интегрированной среде разработки (IDE) Microsoft Visual Studio), которая иллюстрирует алгоритм и результат работы схемы Шнорра, показанные на рисунке 1.

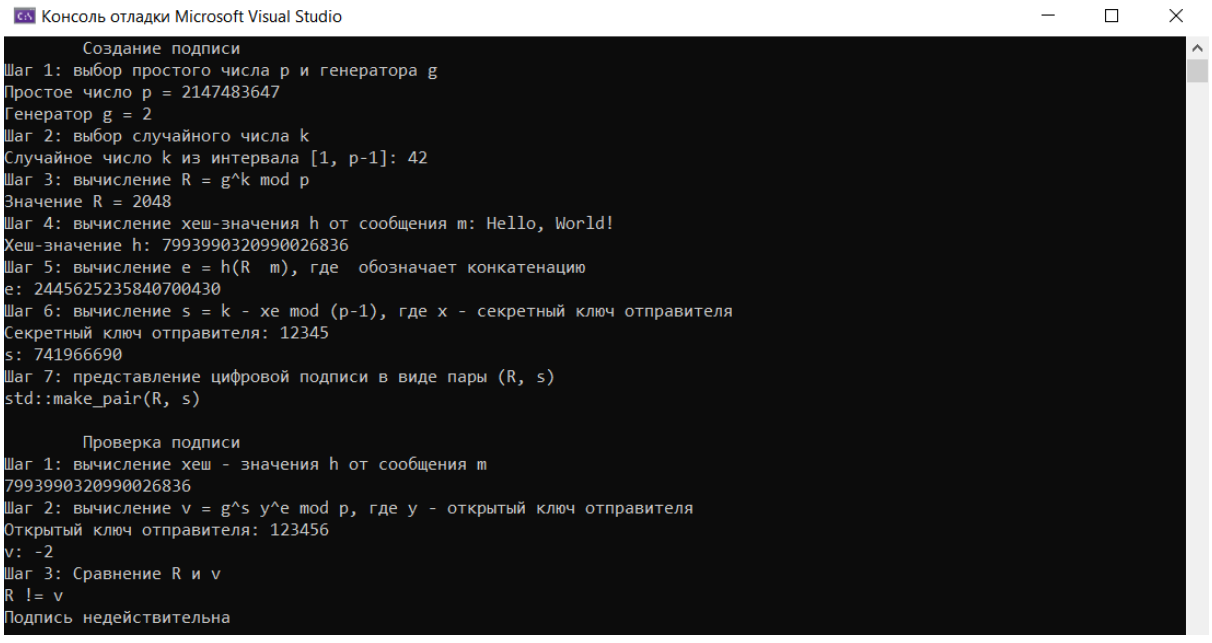

Рисунок 1 -- Результат работы схемы Шнорра на языке программирования C++

Алгоритм разработанного консольного приложения доступен по ссылке (может быть использовано студентами в учебных целях):

- https://github.com/pupajupa/Shnorr-Diagram/tree/main/ShnorrDiagram.

Таким образом, для проверки цифровой подписи схемы Шнорра, получатель должен выполнить три шага: вычислить хеш-значение сообщения, вычислить значение v и сравнить его с

R. Если значения совпадают, то подпись считается действительной. Это обеспечивает целостность и подлинность сообщения и защищает от подделки или изменения данных во время передачи.

Схема Шнорра обладает рядом преимуществ по сравнению с другими протоколами цифровой подписи. Она обеспечивает высокую стойкость к атакам и предотвращает возможность подмены сообщения. Схема Шнорра использует более простой алгоритм, чем ECDSA (Elliptic Curve Digital Signature Algorithm). В ECDSA требуется генерация точек на эллиптической кривой, что требует больше вычислительных ресурсов. Схема Шнорра использует короткие цифровые подписи, что делает ее эффективной и удобной для передачи в цифровых подписях. В схеме Эль-Гамаля и RSA размер подписи значительно больше. Схема Шнорра более безопасна, чем схема Эль-Гамаля и RSA, так как использует случайные числа для генерации подписи, что усложняет возможность атаки методом подбора. Также, при использовании одинаковых длин ключей Схема Шнорра более безопасна, чем ECDSA. Это связано с тем, что алгоритм Схемы Шнорра основан на проблеме дискретного логарифма, которая считается более сложной, чем проблема дискретного логарифма на эллиптических кривых, используемая в ECDSA. Также, в схеме Шнорра используется хэширование сообщения, что защищает от атак с изменением сообщения. В схеме Шнорра используются операции с целыми числами, которые легче вычислять, чем операции с большими простыми числами, которые используются в схемах Эль-Гамаля и RSA. Схема Шнорра обладает более простой структурой и удобнее для использования, поскольку требует меньшего количества вычислений и меньшего объема ключевых материалов. Таким образом, схема Шнорра является более эффективной и безопасной для использования в цифровых подписях, чем схемы Эль-Гамаля и RSA.

Однако у схемы Шнорра есть и недостатки. При использовании одного и того же случайного числа k для нескольких подписей может возникнуть утечка секретного ключа.

Нет защиты от атак на основе квантовых вычислений. В настоящее время схема Шнорра не защищена от атак на основе квантовых вычислений. Если квантовые компьютеры станут доступными в будущем, то это может привести к компрометации подписи, созданной с использованием схемы Шнорра.

Схема Шнорра является одним из наиболее распространенных протоколов цифровой подписи в криптографии. Она обладает высокой стойкостью к атакам и обеспечивает надежную аутентификацию сообщений. Несмотря на некоторые недостатки, она остается одним из самых эффективных способов защиты информации.

Схема Шнорра может использоваться не только для создания цифровых подписей, но и для протоколов аутентификации. Например, она может использоваться для аутентификации пользователей в системах безопасности или для проверки целостности данных в распределенных сетях. Кроме того, схема Шнорра может быть расширена для поддержки мультиподписей, когда несколько участников могут создавать подпись от имени группы. Это может быть полезно, например, для создания мультиподписей в блокчейн-системах.

Одним из интересных свойств схемы Шнорра является ее невосприимчивость к атакам типа "человек посередине" (man-in-the-middle attack). Это связано с тем, что подпись создается на основе хеш-значения сообщения, которое не может быть изменено без изменения самого сообщения.

Наконец, схема Шнорра может быть использована в сочетании с другими криптографическими протоколами, например, для создания безопасных каналов связи или для обеспечения конфиденциальности данных.

Таким образом, схема Шнорра является важным инструментом в области криптографии и находит широкое применение в различных системах безопасности и защиты информации.

Схема Шнорра является одной из наиболее эффективных и теоретически обоснованных схем ЭЦП. На ее основе построен стандарт Республики Беларусь СТБ 1176.2-99, южнокорейские стандарты KCDSA и EC-KCDSA.

Что можно предположить о развитии схемы шнорра в будущем.

С точки зрения криптографии, схема Шнорра уже считается весьма надежным протоколом цифровой подписи. Однако, как и любая другая технология, она может стать устаревшей и уязвимой к новым методам атак.

Возможно, будущее развитие схемы Шнорра будет связано с улучшением ее скорости и эффективности, а также с адаптацией к квантовым вычислениям. Схема Шнорра основана на вычислительной сложности задачи дискретного логарифмирования, которая является одной из задач, которые квантовые компьютеры могут решать гораздо быстрее, чем классические компьютеры. Это означает, что в квантовом мире схема Шнорра может быть легко взломана, если не будут приняты соответствующие меры.

Одним из подходов для адаптации схемы Шнорра к квантовым вычислениям является использование квантовых криптографических протоколов в качестве замены классической схеме.

Например, можно использовать квантовые подписи, такие как подписи на основе определенных квантовых протоколов, например, квантовых ключей.

Другим подходом является использование техник, которые позволяют защитить схему Шнорра от атак квантовых компьютеров. Один из таких подходов - это использование хеш-функций, которые являются устойчивыми к атакам квантовых компьютеров. В этом случае можно использовать хеш-функции на основе квантовых состояний, такие как квантовые хеши, которые используют квантовые свойства для создания устойчивых к атакам квантовых компьютеров хеш-функций.

Также можно использовать кодирование сообщений в квантовом состоянии, которое обеспечивает защиту от перехвата и изменения сообщения. Это может быть достигнуто, например, с помощью квантовых каналов связи.

Таким образом, схема Шнорра может быть адаптирована к квантовым вычислениям, но для этого необходимо принять соответствующие меры для защиты от атак квантовых компьютеров.

Кроме того, существуют и другие протоколы цифровой подписи, которые могут стать более популярными в будущем, например протоколы на основе эллиптических кривых или линейных кодов.

Также возможно, что дальнейший рост схемы Шнорра будет связан с ее использованием в блокчейн-технологиях. Схема Шнорра уже была выбрана в качестве стандарта цифровой подписи для биткоина, и ее использование может распространиться и на другие криптовалюты и блокчейн-проекты.

Однако, как и в любой области технологий, будущее развитие схемы Шнорра будет зависеть от различных факторов, таких как развитие вычислительных возможностей, научных открытий, а также регулятивных и юридических аспектов.

Список использованных источников:

1.Geeks for Geeks, Цифровая подпись Шнорра [Электронный ресурс]. – Режим доступа: https://www.geeksforgeeks.org/schnorr-digital-signature/.

2. Википедия, Схема Шнорра [Электронный ресурс]. – Режим доступа: https://en.wikipedia.org/wiki/Schnorr_signature.

3.Хабр, Схема Шнорра и её роль в Биткоине [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/534306/.

4.Tari Labs University, Основы подписи Шнорра [Электронный ресурс]. – Режим доступа: https://tlu.tarilabs.com/cryptography/introduction-schnorr-signatures#basics-of-schnorr-signatures.