УДК 003.09

Абдиев Е. Е.
магистрант, 1 курс,
факультет «Технологический»
Казахский университет технологии и бизнеса
им. К. Кулажанова» Казахстан, г. Астана
Жантлесов Е. Ж.
доктор философии
кафедры «Информационные системы»,
Казахский университет технологии и бизнеса
им. К. Кулажанова» Казахстан, г. Астана
Кульмамиров С. А.
кандидат экономических наук,
ассистент профессора кафедры «Информационные системы»,
Казахский университет технологии и бизнеса
им. К. Кулажанова» Казахстан, г. Астана

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ РЕАЛИЗОВАННОГО КРИПТОГРАФИЧЕСКОГО ПРОТОКОЛА ЦИФРОВОЙ ПОДПИСИ ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ

Аннотация. *В статье рассматривается криптографический протокол цифровой подписи на основе эллиптических кривых. Осуществлен анализ криптографической стойкости протокола. Построен график зависимости криптографической стойкости протокола от характеристики поля с построением эллиптических кривых. Реализована программа, поддерживающая библиотеки больших чисел GMP. Полученное программное*

приложение может стать инструментом, позволяющим передавать и получать сообщения с хорошей криптографической стойкостью и приемлемой скоростью.

Ключевые слова: *криптография, криптографический протокол, эллиптические кривые, криптографическая стойкость.*

Annotation. *The article discusses a cryptographic digital signature protocol based on elliptic curves. The cryptographic strength of the protocol is analyzed. A graph of the dependence of the cryptographic strength of the protocol on the characteristics of the field with the construction of elliptic curves is constructed. A program has been implemented that supports libraries of large GMP numbers. The resulting software application can become a tool that allows you to send and receive messages with good cryptographic strength and acceptable speed.*

Keywords: *cryptography, cryptographic protocol, elliptic curves, cryptographic strength.*

Введение

В современном мире быстрыми темпами растет тенденция всестороннего развития технологий и мощностей вычислительных систем высокоскоростных компьютеров. Тем самым расширяя возможности персональных компьютеров и суперкомпьютеров. В связи с этим, возникла необходимость модернизации существующих средств защиты информации. Как показывает практика используемые на сегодняшний день криптографические протоколы, показывающие достаточную стойкость ко взлому, уже быстро взламываются криптоаналитиками.

Перед специалистами встает задача разработки новых протоколов с большей вычислительной сложностью для устранения и ликвидации попытки обойти или нарушить безопасность криптографического протокола. Для решения данной задачи в современной криптографии широко используется одна

из областей теории чисел и алгебраической геометрии - теория эллиптических кривых над конечными полями. В криптографии пока не существует алгоритмов субэкспоненциальной сложности для взлома таких систем.

Целью настоящей статьи является разработать свой криптографический протокол для получения лучших результатов криптографической стойкости передающих сообщений по каналам телекоммуникаций. Предусмотрена возможность поддержки библиотеки больших чисел GMP [1].

Приложение, созданное в результате разработки, имеет потенциал стать средством для обеспечения передачи и приема сообщений с необходимым уровнем криптографической стойкостью. Оно предоставляет возможность использовать его как альтернативу уже существующим криптографическим протоколам.

Основная часть.

1. Криптографические протоколы.

Протокол - это распределенный алгоритм, в процессе выполнения которого два участника последовательно обмениваются сообщениями [2].

Криптографический протокол представляет собой набор инструкций, предназначенных для обеспечения работы криптографической системы, в которой участники взаимодействия используют специальные криптографические методы. Эта система обеспечивает защиту информации при ее передаче и обмене между участниками.

Стойкость криптографических систем определяется их способностью выдерживать атаки со стороны злоумышленников, которые стремятся подорвать безопасность функций системы и завладеть секретным ключом.

При рассмотрении протоколов передачи сообщений и цифровой подписи на основе эллиптических кривых рассматривается устойчивость

криптографических протоколов к атакам противника. Злоумышленник в данном случае - это субъект, который наблюдает за передаваемым сообщением, перехватывает, искажает, модифицирует, вставляет, повторяет или перенаправляет сообщение, тем самым вмешиваясь в работу служб безопасности криптографической системы.

Функция - это сервис защиты безопасности, выполняемая подсистемой безопасности. Криптографические системы обеспечивают функции безопасности с помощью криптографических протоколов.

Ниже перечислены требования к протоколу, необходимые для передачи сообщений:

- аутентификация источника данных, здесь проверяется, что передаваемый документ был создан указанным источником;

- обеспечение целостности данных, что исключает возможность внесения изменений после создания документа.

Задачей аутентификации источника данных применяется схема цифровой подписи сообщения [2].

2. Протокол передачи сообщений на основе эллиптических кривых.

Опишем разработанный протокол передачи сообщений с использованием базиса эллиптических кривых. Алгоритм передачи сообщения M от пользователя A (отправителя) к пользователю B (получателю) описан пошагово ниже:

Шаг 1. Подписываем передаваемое сообщение цифровой подписью Шнорра [2], используя хэш-функцию Tiger [4-6];

Шаг 2. Выбираем эллиптическую кривую и точку на ней для применения в шифровании передаваемых данных (метод случайного выбора) [3];

Шаг 3. Полученное сообщение (текст в виде ASCII-кодов) представим в виде точки на эллиптической кривой (способ представления - вероятностный метод представления открытого текста) [3];

Шаг 4. К точке, полученной на шаге 3, применим систему шифрования Эль-Гамаля для эллиптических кривых [3];

Шаг 5. Откроем общий доступ к каналу связи оценив:

- характеристику поля;

- найденную эллиптическую кривую;

- точку, выбранную на эллиптической кривой (шаг 2);

- открытый ключ отправителя сообщения;

- открытый ключ цифровой подписи;

Шаг 6. Зашифрованное сообщение передается по открытому каналу связи;

Шаг 7. Получатель расшифровывает сообщение и проверяет правильность цифровой подписи;

Шаг 8. Если цифровая подпись не верна, сообщение игнорируется.

Данный алгоритм обладает следующими свойствами:

- криптографический протокол цифровой подписи представляет собой систему с не доверяющими друг другу сторонами, в которой используются бесключевые хэш-функции;

- бесключевая хэш-функция Tiger не имеет патентных ограничений, достаточно устойчива к атакам, совместима с современными хэш-функциями с высокой скоростью работы.

Такая схема цифровой подписи является одноразовой. В настоящее время широко применяются криптографические системы с открытым ключом в различных сетевых протоколах.

Схема Шнорра одна из наиболее эффективных среди практических протоколов аутентификации, реализующая данную задачу. Она минимизирует зависимость вычислений, необходимых для создания подписи, от сообщения.

Цифровая подпись Шнорра - ассиметричная цифровая подпись с открытым ключом. Эта подпись имеет ряд преимуществ:

- схема основана на сложности вычисления значения логарифма в конечном поле;

- достоинством такой схемы цифровой подписи является в том, что один секретный ключ может генерировать подписи для большого количества сообщений;

- при попытке компрометации схемы сталкивается с решением сложной математической задачи, такой как вычисление значения логарифма в простом конечном поле;

- при использовании данной схемы невозможно обнаружить использование повторно случайного числа;

- введение в алгоритм простого числа позволяет сократить длину цифровой подписи.

Новый протокол использует формирование цифровой подписи и позволит шифровать передаваемые сообщения на основе эллиптических кривых. Этот метод усилит криптографическую стойкость используемой системы. В результате, если злоумышленник перехватит сообщение, расшифровать данные станет еще сложнее.

Для шифрования используется система Эль-Гамаля [5]. Система работает с менее трудоемким алгоритмом, меньшей вероятностью перехвата сообщения, большей пропускной способностью канала связи.

При выборе кривой и точки используется случайный выбор [4-5]. Для реализации криптографического протокола описанный алгоритм обладает хорошими характеристиками быстродействия.

Представление открытого текста осуществляется вероятностным методом [6]. Здесь используется алгоритм с малой вероятностью неудачи. Во всех рассмотренных алгоритмах использованы ассиметричные системы шифрования.

3. Проверка устойчивости протокола к атакам средствами AVISPA.

Для проверки созданного протокола на устойчивость к атакам противника применен пакет AVISPA [7].

Пакет AVISPA интегрирует все современные подходы к анализу протоколов: проверка на модели, древовидные автоматы, временная логика. Имеются версии языков для описания протоколов, что расширяет классификацию изучаемых протоколов. Создаваемые протоколы интегрируются в единую платформу [1, 7].

Созданный протокол исследован в программе на языке CAS+ [7], который описывает сеанс связи построенного протокола. Далее пакетом SPAN исследуемое программное приложение переведено в формализованный язык описания протоколов HLPSL (или язык IF). Это позволило получить результаты проверки устойчивости протокола к атакам в среде AVISPA.

В результате проверки протокола имеющихся атак на протокол не обнаружено. Однако, злоумышленник может получить доступ к информации, решив задачу дискретного логарифма на эллиптической кривой (рисунок 1).

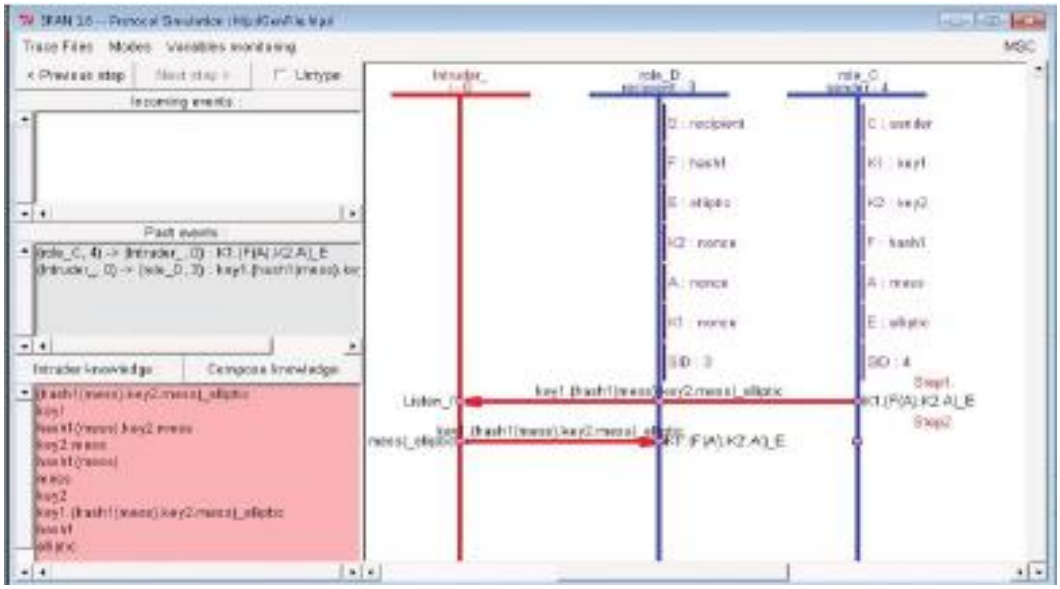

Рисунок 1

Результат проверки протокола средствами AVISPA.

Злоумышленник (Intruder) и его знания показаны внизу слева

4. Анализ стойкости криптографического протокола на основе эллиптических кривых.

Важно проводить криптографический анализ новейших криптографических алгоритмов. В результате можно проанализировать и выявить, что исследуемый криптографический алгоритм нестабилен. Это позволит своевременно улучшить протокол или заменить его на новый.

Таким образом, надежность цифровой подписи определяется стойкостью к криптоаналитическим атакам двух ее компонент: хэш-функции и самого алгоритма цифровой подписи [8].

В исследуемом протоколе использовали хэш-функцию Tiger. Атака на Tiger-24 выявила псевдоколлизию со сложность 247 операций до взлома с применением 192-битное хэш значение [6]. Стойкость алгоритма цифровой подписи для построенного протокола анализировалась стойкостью цифровой

подписи Шнорра, а также шифрованием по системе Эль-Гамаля на эллиптических кривых [5].

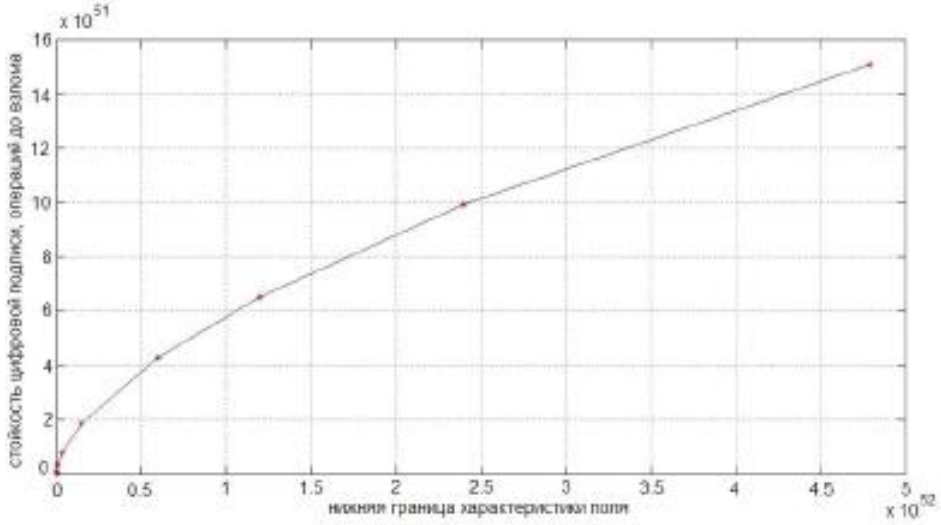

Рисунок 2

Зависимость стойкости протокола цифровой подписи от нижней границы характеристики поля

График зависимости стойкости протокола от нижней границы характеристики поля, начиная с 160 бит, приведен на рисунке 2.

Стойкость цифровой подписи Шнорра определяется сложностью решения задачи дискретного логарифма. Сейчас самым быстрым алгоритмом, решающим эту задачу, является алгоритм обобщенного решета числового поля [8]. При характеристике поля порядка 160 бит, стойкость составляет $1,8\times10^{11}$ операций до взлома. Следует отметить, что наиболее быстрыми алгоритмами решения задачи дискретного логарифма в группе точек эллиптической кривой считаются l-метод Полларда [9]. При характеристике поля порядка 160 бит стойкость составляет $1,94\times10^{26}$ операций до взлома [2, 9].

Заключение. Таким образом, криптографическая стойкость построенного протокола составила 5×10^{51} раз. Известно, что криптографическая стойкость ГОСТ Р 34. 10-2001 криптографического протокола цифровой подписи, наиболее близкого к алгоритму, составляет 1,93×1035 раз. В настоящее время применяется схема цифровой подписи с характеристикой поля 256 двоичных разрядов, ее стойкость составляет 3,02×1038 операций до взлома [10].

В Республике Казахстан на сегодняшний день используется, генерация открытых и закрытых ключей Национального удостоверяющего центра Республики Казахстан производится на алгоритмах RSA и ГОСТ 34.310-2004. Учитывая, что информационные технологии и методы криптографического анализа непрерывно развиваются, планируется осуществить переход на криптографический стандарт СТ РК ГОСТ Р 34.10-2015, тем самым повысив криптографическую стойкость.

Список использованных источников:

1. The GNU Multiple Precision Arithmetic Library. - http: //gmplib.org.

2. Черемушкин А. В. Криптографические протоколы: основные свойства и уязвимости / А. В. Черемушкин. - М.: Академия, 2009.

3. Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц. - М.: ТВП, 2001.

4. Tiger: a Fast New Cryptographic Hash Function (Designed in 1995). - http://www.cs .technion. ac.il/biham/Reports/Tiger.

5. Mendel F. Cryptanalysis of the Tiger Hash Function / F. Mendel, V. Rijmen. – Springer Berlin; Heidelberg: ASIACRYPT, 2007.

6. AVISPA - http://www. avispa-project .org.

7. Алгоритмические основы эллиптической криптографии / А. А. Болотов, С. Б. Гашков, А. Б. Фролов, А. А. Часовских. - М: МЭИ, 2000.

8. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин - М.: Радио и связь, 2001.

9. Бондаренко М. Ф. Сущность и результаты исследований свойств перспективных стандартов цифровой подписи X9.62- 1998 и распределения ключей X9.63 - 199X на эллиптических кривых / М. Ф. Бондаренко, И. Д. Горбенко, Е. Г. Качко. // Радиотехника. – 2000 - 114. С. 15-24.