https://doi.org/10.31643/2018.050
22 November 2018

Кульмамиров Серик Алгожаевич, к.т.н, академик МАИН
E-mail: kaznukulma@mail.ru ORCID ID 0000-0003-0912-7836
Акшолак Гулнур Исатайкызы, магистрант
E-mail: gulnuraqsholaq@gmail.com ORCID ID 0000-0001-8292-6939
Казахский национальный университет имени аль-Фараби
г. Алматы, Казахстан

АНАЛИЗ ШИФРОВАННЫХ АЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Kulmamedov Serik, Candidate of Engineering Sciences
E-mail: kaznukulma@mail.ru ORCID ID 0000-0003-0912-7836
Aksholak Gulnur, Master's Degree student
E-mail: gulnuraqsholaq@gmail.com ORCID ID 0000-0001-8292-6939
Al-Farabi Kazakh National University
Almaty, the Republic of Kazakhstan

ANALYSIS OF ENCRYPTED DIGITAL SIGNATURE ALGORITHMS BASED ON ELLIPTIC CURVES

Annotation: *The article discusses cryptographic algorithms based on elliptic curves over finite fields. It is shown that elliptic curves allow us to construct examples of finite abelian groups for cryptographic purposes. By evaluating the field, you can easily increase the cipher strength. A variant of the software implementation of this approach is considered. A software-implemented protocol can encrypt messages, generate a digital signature, and after transmitting the message, decrypt them on the recipient's side. The evaluation of the cryptographic strength of the described protocol was made.*

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

Аннотация: *В статье рассматриваются криптографические алгоритмы, базирующиеся на эллиптических кривых над конечными полями. Показано, что эллиптические кривые позволяют строить примеры конечных абелевых групп для криптографических целей. Оценкой поля можно легко повышать стойкость шифра. Рассмотрен вариант программной реализации такого подхода. Программно реализованный протокол может шифровать сообщения, формировать цифровую подпись, после передачи сообщения расшифровать их на стороне получателя. Произведена оценка криптографической стойкости описываемого протокола.*

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

В наше время повсеместно используются криптографические алгоритмы или протоколы, которые базируются на эллиптических кривых над конечными полями [10]. Общеизвестно, что эллиптические кривые позволяют строить примеры конечных абелевых групп с хорошими, для криптографических целей, параметрами [9]. Меняя характеристику поля можно легко повышать стойкость шифра. Поэтому существенную роль играет возможность удобной программной реализации такого алгоритма [1]. Такой программно реализованный криптографический протокол цифровой подписи на основе эллиптических кривых будет всеобще востребован. Протокол производит шифрование сообщения, формирование цифровой подписи, передачу сообщения и расшифровку на стороне получателя. Необходимо проводить исследования по оценке криптографической стойкости такого протокола.

https://doi.org/10.31643/2018.050
22 November 2018

Данная статья посвящена к этим задачам и проблемам в ходе реализации таких задач. В итоге получена зависимость криптографической стойкости протокола от характеристики конечного поля, над которым строится эллиптическая кривая [2].

Также обсуждается вариант реализации программы, производящей шифрование и дешифрование сообщения в соответствии с построенным протоколом [7]. Такая программа может стать инструментом передачи или получения сообщения с достаточной степенью криптографической стойкости и приемлемой скоростью.

Таким образом, в связи с возрастающей вычислительной мощностью компьютеров разного класса возникает необходимость модернизации существующих средств защиты информации. Криптографические протоколы, показывающие достаточную стойкость к взлому, с каждым днем взламываются все быстрее. Хотя современные криптографические протоколы работают эффективно, но все же нужно задумываться о построении протоколов с большей вычислительной сложностью задачи взлома. Поэтому в криптографии начали все больше применять современные решения теории чисел и алгебраической геометрии теории эллиптических кривых над конечными полями [1, 6].

Эллиптические кривые над конечными полями доставляют неисчерпаемый источник конечных абелевых групп, которые удобны для высокопроизводительных вычислений и обладают расширенной структурой. Преимуществами криптосистем на эллиптических кривых являются наличие субэкспоненциальных алгоритмов вскрытия криптосистем, если в них не используются суперсингулярные кривые вида $y^2 + y = x^3 + ax + b$ [3-4].

Цель нашей статьи – описать криптографический протокол, позволяющий добиться лучших результатов криптостойкости, чем существующие протоколы цифровой подписи и передачи сообщений на эллиптических кривых.

Криптографический протокол является распределенный алгоритм, в процессе выполнения которого два участника последовательно выполняют определенные действия и обмениваются сообщениями [6-7]. Такой протокол предназначен для выполнения функций системы шифрования сообщений. В процессе его выполнения участники используют криптографические алгоритмы. Криптографическая система обеспечивает уровень безопасности информации криптографическими методами [5].

В основе выбора и построения криптографических систем лежит условие обеспечения криптографической стойкости. Под стойкостью криптографических систем понимают их способность противостоять атакам противника или нарушителя, имеющим целью нейтрализацию нескольких функций безопасности, а также получению секретного ключа. При рассмотрении протоколов передачи сообщений и цифровой подписи на основе эллиптических кривых следует рассматривать стойкость криптографического протокола к атакам противника.

Противником является внешний субъект, наблюдающий за передаваемыми сообщениями. Он также захочет вмешиваться в работу участников различными путями: перехват сообщения; искажения (модификации) сообщении; вставки (создания новых) сообщения; повтора и перенаправления сообщений; блокирования передачи в целях нарушения функций сервисов безопасности.

Опишем теперь протокол передачи сообщений на основе эллиптических кривых: при передаче сообщения M от пользователя A (т.е. отправителя) к пользователю B (получателю) реализовываются следующие шаги:

Шаг 1. Подписывается передаваемое сообщение цифровой подписью Шнорра [9], используя хэш-функцию Tiger [2-4] в соответствующих шагах алгоритма подписи.

Шаг 2. Выбирается эллиптическая кривая и точка на ней для последующего использования в шифровании. Здесь можно применить метод случайного выбора [1];

https://doi.org/10.31643/2018.050
22 November 2018

Шаг 3. Полученное сообщение представляется в виде точки на эллиптической кривой. Для этого удобно использовать вероятностный метод представления открытого текста [1]. При этом текст представляется в виде ASCII-кодов символов.

Шаг 4. К этой точке следует применить аналог системы шифрования Эль-Гамаля для эллиптических кривых [1].

Шаг 5. В канале связи установим общедоступность следующим параметрам: характеристика поля; определенную над ним эллиптическую кривую; точка, выбранная на шаге 2; открытый ключ отправителя сообщения; открытый ключ цифровой подписи;

Шаг 6. По открытому телекоммуникационному каналу передается зашифрованное сообщение.

Шаг 7. Получатель по общедоступным данным расшифровывает сообщение и удостоверяется в правильности цифровой подписи.

Шаг 8. В случае неверной цифровой подписи сообщение игнорируется.

Так как схемы цифровой подписи на основе симметричных систем шифрования являются по существу одноразовыми, то для формирования цифровой подписи следует использовать систему шифрования с открытым ключом [7]. К услугам доверенной третьей стороны прибегать не рекомендуется, поскольку это связано с дополнительными сложностями реализации и негативно влияет на безопасность протокола в целом.

Цифровая подпись Шнорра является ассиметричной цифровой подписью с открытым ключом [3-4]. Она является цифровой подписью на основе специально разработанного алгоритма. Эта подпись имеет ряд преимуществ по сравнению с объединенными подходами к построению цифровых подписей. Перечислим их:

- схема основана на сложности вычисления значения логарифма в конечном поле. Достоинством схемы является возможность выработки подписей для большого числа сообщений с использованием одного секретного ключа;

- при использовании этой схемы нельзя обнаружить повторное использование случайного числа. Повторяющиеся значения γ спрятаны в значение хэш-функции. Поэтому для разных сообщений значения первых компонент подписи почти всегда будут различными;

- введение в алгоритм простого числа позволяет сократить длину подписи по сравнению с подписями, основанными на сложности вычисления логарифма в конечном поле.

При построении протокола нужно использовать не только цифровую подпись, но и шифрование самого передаваемого сообщения на эллиптических кривых. Этот способ усилит криптографическую стойкость системы. Такой алгоритм при перехвате сообщения злоумышленником позволит создать дополнительные трудности при взломе или подмене информации.

Для шифрования выбирается система шифрования Эль-Гамаля. Она отличается от остальных существующих систем шифрования на эллиптических кривых: менее трудоемким алгоритмом; меньшей вероятностью перехвата сообщения; большей пропускной способностью телекоммуникационного канала.

При этом стойкость системы не уменьшается, поскольку она основана на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой.

Во всех описанных алгоритмах используются ассиметричные системы шифрования, что позволит получить дополнительную защиту протокола [5].

Для проверки протокола на устойчивость к атакам противника используется пакет AVISPA [8]. Продукт AVISPA интегрирует все современные подходы к анализу протоколов: проверка на модели, древовидные автоматы, временная логика. Проверку протокола можно реализовать составлением программы на языке CAS+. Далее средствами пакета SPAN создаваемую

https://doi.org/10.31643/2018.050
22 November 2018

программу можно перевести в формализованный язык описания протоколов HLPSL. Также есть возможность получения программы на низкоуровневом языке типа IF, по которому возможно получение результатов проверки устойчивости протокола к атакам средствами AVISPA [8].

Проведенные исследования показали, что в результате проверки протокола известных атак не найдено. Злоумышленник может получить доступ к информации, только решив задачу дискретного логарифмирования на эллиптической кривой. Действия злоумышленника после сеанса протокола показаны на рисунке 1 [8].

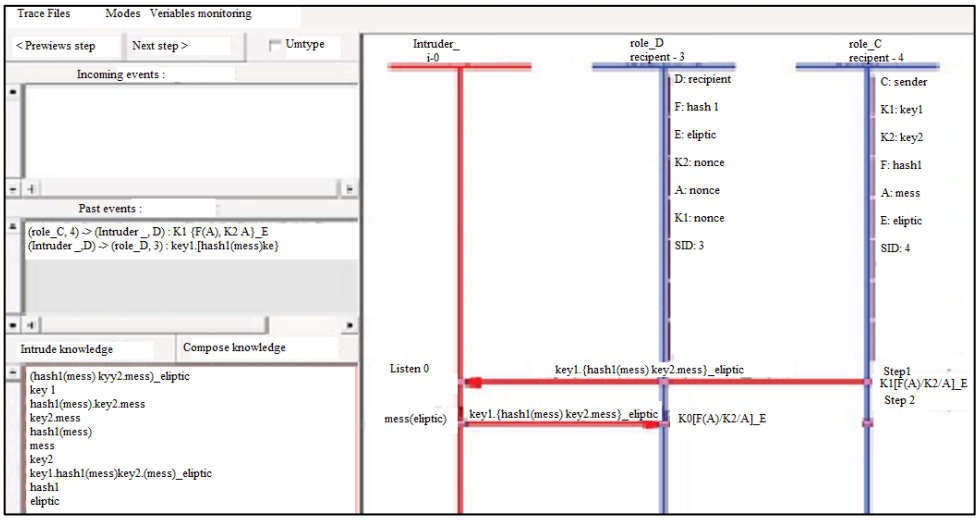

Рисунок 1. Результат проверки протокола средствами AVISPA: действия злоумышленника (Intruder) видны на графике внизу слева

Таким образом, проведение криптоанализа для давно существующих и недавно появившихся криптоалгоритмов очень актуально, так как оперативно можно заключить, что исследуемый криптоалгоритм нестоек и необходимо его усовершенствовать. Или следует его заменить новым алгоритмом.

Надежность цифровой подписи определяется стойкостью к криптоаналитическим атакам двух ее компонент: хэш-функции и самого алгоритма ЭЦП [7]. В нашем исследовании использована хэш-функция Tiger [3]. Атака на Tiger-24 дает почти псевдоколлизию со сложность 247 операций до взлома, при этом используется 192-битное хэш-значение [4]. Стойкость алгоритма цифровой подписи для построенного протокола определяется стойкостью цифровой подписи Шнорра и шифрованием по системе Эль-Гамаля на эллиптических кривых [9].

Стойкость цифровой подписи Шнорра основана на сложности решения задачи дискретного логарифмирования в простом конечном поле. На сегодняшний день самым быстрым алгоритмом, решающим эту задачу, является алгоритм обобщенного решета числового поля [6-7]. При характеристике поля порядка 160 двоичных разрядов (бит) стойкость составляет 1, 8 · 1011 операций до взлома.

В настоящее время наиболее быстрыми алгоритмами решения задачи дискретного логарифмирования в группе точек эллиптической кривой при правильном выборе параметров считаются *r*-метод и *l*-метод Полларда [6]. Например, для улучшенного *r*-метода Полларда вычислительная сложность оценивается в следующем: при характеристике поля порядка 160 бит стойкость составляет 1,94 · 1026 операций до взлома.

https://doi.org/10.31643/2018.050
22 November 2018

Для обеспечения необходимого уровня стойкости построенного протокола должно выполняться ограничение на характеристику поля: она должна быть более 160 бит [6, 9]. Никаких других ограничений на параметры протокола не накладывается ввиду надежности применяемых методов и алгоритмов.

Таким образом, криптографическая стойкость построенного протокола в худшем случае (при значении характеристики поля 160 бит) составляет 5 · 1051 операций до взлома.

В настоящее время применяется схема ЭЦП ГОСТ Р34.10-2001 с характеристикой поля 256 двоичных разрядов, ее стойкость составляет 3,02 · 1038 операций до взлома [5].

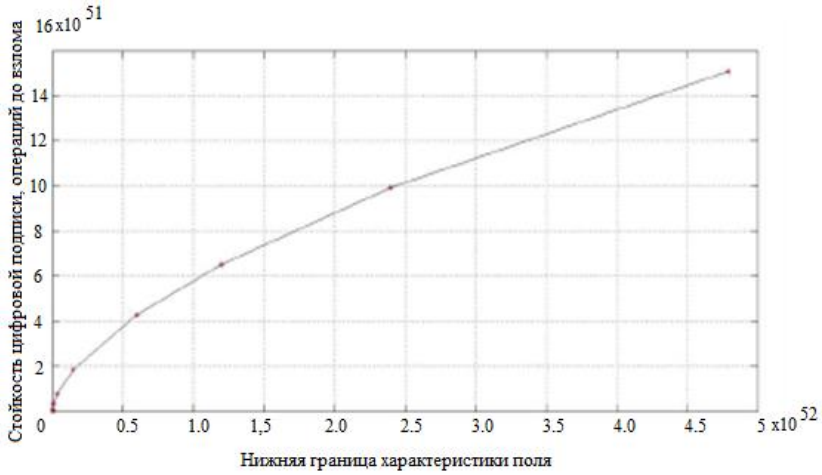

Рисунок 2. Зависимость стойкости протокола цифровой подписи от нижней границы характеристики поля

График зависимости стойкости криптопротокола от нижней границы характеристики поля, начиная с 160 бит, приведен на рисунке 2 (кривая позаимствована с источника [9]).

ЛИТЕРАТУРА

1. Коблиц Н. Курс теории чисел и криптографии. – М.: ТВП, 2001. – 254 с.
2. Kelsey J . Collisions and Near-Collisions for Reduced-Round Tiger, Proceedings of Fast Software Encryption. - Graz : FSE, 2006.
3. Tiger: a Fast New Cryptographic Hash Function. 1995. – URL: http://www.cs.technion. ac.il/biham/Reports/Tiger (дата обращения 12.10.2018).
4. Mendel, F . Cryptanalysis of the Tiger Hash Function. – Springer Berlin; Heidelberg: ASIACRYPT, 2007.
5. Романец Ю. В. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 2001. – 376 с.
6. 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.: Радиотехника. – 2000.
7. Алгоритмические основы эллиптической криптографии / А. А. Болотов, С. Б Гашков, А. Б. Фролов, А. А. Часовских. - М: МЭИ, 2000.
8. AVISPA. – URL: http://www. avispa-project .org (дата обращения 12.10.2018).
9. The GNU Multiple Precision Arithmetic Library. – URL: http://gmplib.org. (дата обращения 10.10.2018).
10. Черемушкин А. В. Криптографические протоколы: основные свойства и уязвимости. – М.: Академия, 2009. – 272 с.