УДК 003.26(075.8)

РАЗРАБОТКА, РЕАЛИЗАЦИЯ И АНАЛИЗ КРИПТОГРАФИЧЕСКОГО ПРОТОКОЛА ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

С.Г. Чеканов

В последнее время широкое распространение получили криптографические примитивы, которые базируются на эллиптических кривых над конечными полями. Основная причина этого заключается в том, что эллиптические кривые позволяют строить примеры конечных абелевых групп с хорошими, для криптографических целей параметрами. Кроме того, меняя характеристику поля можно легко повышать стойкость шифра. Существенную роль играет возможность удобной программной реализации. Разработан и программно реализован криптографический протокол цифровой подписи на основе эллиптических кривых. Протокол производит шифрование сообщения, формирование цифровой подписи, передачу сообщения и расшифровку на стороне получателя. Проанализирована криптографическая стойкость протокола несколькими методами. Построен график зависимости криптографической стойкости протокола от характеристики конечного поля, над которым строится эллиптическая кривая. Написана программа на языке C++ в среде программирования Visual C++ 2010 с поддержкой библиотеки больших чисел GMP, производящая шифрование и дешифрование сообщения в соответствии с построенным протоколом. Разработанная программа является инструментом, позволяющим передавать и получать сообщения с достаточной степенью криптографической стойкости и приемлемой скоростью.

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

Введение

В настоящее время наблюдается тенденция быстрого развития технологий и мощностей вычислительных систем компьютеров. У современных компьютеров повышается производительность за счет использования новых материалов в изготовлении, за счет улучшения взаимодействия между частями электронно-вычислительной машины, и т.п. Расширяются возможности персональных компьютеров и суперкомпьютеров. В связи с возрастающей вычислительной мощностью ЭВМ возникает необходимость модернизации существующих средств защиты информации. Криптографические протоколы, показывающие достаточную стойкость ко взлому сегодня, с каждым днем взламываются все быстрее. Несмотря на то, что современные криптографические протоколы могут эффективно работать еще достаточное количество времени, стоит задумываться о построении протоколов с большей вычислительной сложностью задачи взлома. В последнее время для решения этого вопроса в криптографии нашла применение одна из областей теории чисел и алгебраической геометрии – теория эллиптических кривых над конечными полями. Основная причина этого состоит в том, что эллиптические кривые над конечными полями доставляют неисчерпаемый источник конечных абелевых групп, которые (даже если они велики) удобны для вычислений и обладают богатой структурой. Преимущества криптосистем на эллиптических кривых заключается в том, что неизвестны субэкспоненциальные алгоритмы вскрытия этих систем, если в них не используются суперсингулярные кривые (вида $y^2 + y = x^3 + ax + b$), а также кривые, порядки которых (число различных точек на кривой) делятся на большое простое

число. Цель статьи – описание разработанного и реализованного собственного криптографического протокола, позволяющего добиться лучших результатов криптостойкости, чем существующие протоколы цифровой подписи и передачи сообщений на эллиптичсеких кривых. Написана программа на языке C++ в среде программирования Visual C++ 2010 с поддержкой библиотеки больших чисел GMP [1], производящая шифрование и дешифрование сообщения в соответствии с построенным протоколом. Разработанная программа является инструментом, позволяющим передавать и получать сообщения с достаточной степенью криптографической стойкости и приемлемой скоростью. Существование такого программного продукта позволяет в будущем использовать его в качестве альтернативы известным криптографическим протоколам.

1. Криптографические протоколы

Протокол – распределенный алгоритм, в процессе выполнения которого два (или более) участника последовательно выполняют определенные действия и обмениваются сообщениями.

Криптографический протокол – протокол, предназначенный для выполнения функций криптографической системы; в процессе его выполнения участники используют криптографические алгоритмы. В данном случае под *криптографической системой* понимают систему обеспечения безопасности информации криптографическими методами.

В основе выбора и построения криптографических систем лежит условие обеспечения криптографической стойкости. Под *стойкостью* криптографических систем понимают их способность противостоять атакам противника и (или) нарушителя, как правило, имеющим целью нейтрализацию одной или нескольких функций безопасности и, прежде всего, получение секретного ключа.

При рассмотрении протоколов передачи сообщений и цифровой подписи на основе эллиптических кривых будем рассматривать стойкость криптографического протокола к атакам противника.

Противник – внешний субъект (или коалиция субъектов), наблюдающий за передаваемыми сообщениями и, возможно, вмешивающийся в работу участников путем перехвата, искажения (модификации), вставки (создания новых), повтора и перенаправления сообщений, блокирования передачи в целях нарушения одной или нескольких функций - сервисов безопасности.

Функция – сервис безопасности – защитная функция, выполняемая подсистемой безопасности и определяемая ее целевым назначением.

Поскольку криптографическая система может обеспечивать различные функции безопасности, для реализации которых применяют разнообразные криптографические протоколы, то и свойств, характеризующих безопасность криптографического протокола, также достаточно много. Обычно свойства протоколов, характеризующие их стойкость к различным атакам, формулируют как цели или требования к протоколам.

Наиболее важные требования к протоколу при передаче сообщений следующие:

аутентификация источника данных – получение подтверждения того, что рассматриваемый документ был создан именно указанным источником информации (без установления времени создания и единственности документа);

обеспечение целостности данных , т.е. невозможности их модификации после создания. Можно рассматривать как часть задачи аутентификации источника данных [2].

Для реализации современных протоколов с заявленными требованиями успешно применяется схема цифровой подписи сообщения.

2. Протокол передачи сообщений на основе эллиптических кривых

Теперь перейдем непосредственно к описанию разработанного протокола передачи сообщений на основе эллиптических кривых. При передаче сообщения M от пользователя A (отправителя) к пользователю B (получателю) выполняются следующие шаги:

1) подписываем передаваемое сообщение цифровой подписью Шнорра [2], используя хэш-функцию Tiger [4–6] в соответствующих шагах алгоритма подписи;

2) выбираем эллиптическую кривую и точку на ней для последующего использования в шифровании. Используем метод случайного выбора [3];

3) полученное сообщение представляем в виде точки на эллиптической кривой, используя вероятностный метод представления открытого текста [3]. При этом текст представляется в виде ASCII-кодов символов;

4) к точке, полученной на шаге 3, применяем аналог системы шифрования Эль-Гамаля для эллиптических кривых [3];

5) делаем общедоступными в канале связи:

характеристику поля;

определенную над ним эллиптическую кривую;

точку, выбранную на шаге 2;

открытый ключ отправителя сообщения;

открытый ключ цифровой подписи;

6) передаем по открытому каналу связи зашифрованное сообщение;

7) получатель по общедоступным данным расшифровывает сообщение и удостоверяется в правильности цифровой подписи;

8) в случае неверной цифровой подписи сообщение игнорируется.

Выбор данных алгоритмов обусловлен следующими соображениями:

Для криптографических протоколов цифровой подписи, которые являются системами с не доверяющими друг другу сторонами необходимо использовать бесключевые хэш-функции.

Бесключевая хэш-функция Tiger не имеет патентных ограничений, имеет достаточную устойчивость к атакам, совместима с большинством современных хэш-функций (удобство модификации), имеет высокую скорость работы.

Так как схемы цифровой подписи на основе симметричных систем шифрования являются по существу одноразовыми, для формирования цифровой подписи будем использовать систему шифрования с открытым ключом. К услугам доверенной третьей стороны прибегать не будем, поскольку это связано с дополнительными сложностями реализации и негативно влияет на безопасность протокола в целом. Цифровая подпись Шнорра – ассиметричная цифровая подпись с открытым ключом. Она является цифровой подписью на основе специально разработанного алгоритма, поэтому имеет ряд преимуществ по сравнению с объединенными подходами к построению цифровых подписей:

– схема основана на сложности вычисления значения логарифма в конечном поле. Основным достоинством такой схемы цифровой подписи является возможность выработки цифровых подписей для большого числа сообщений с использованием одного секретного ключа. При этом попытка компрометации схемы сталкивается с необходимостью решения сложной математической задачи, связанной с нахождением решений показательных уравнений, в частности с нахождением значения логарифма в простом конечном поле;

– при использовании данной схемы нельзя обнаружить повторное использование случайного числа, проверяя совпадение первых компонент цифровой подписи, как это возможно, например, для схемы цифровой подписи Эль-Гамаля, основу которой также составляет

сложность вычисления логарифма в конечном поле. Повторяющиеся значения γ спрятаны в значение хеш-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 будем использовать не только цифровую подпись, но и шифрование самого передаваемого сообщения на эллиптических кривых, чтобы усилить криптографическую стойкость системы. Такой порядок действий позволяет при перехвате сообщения злоумышленником создать дополнительные трудности при взломе или подмене информации.

Для шифрования выберем систему Эль-Гамаля, которая выгодно отличается от остальных существующих систем шифрования на эллиптических кривых менее трудоемким алгоритмом, меньшей вероятностью перехвата сообщения, большей пропускной способностью канала связи. При этом стойкость системы не уменьшается, поскольку она основана на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой.

При выборе кривой и точки будем использовать случайный выбор, поскольку для реализации протокола этот алгоритм подходит и обладает достаточно хорошими характеристиками быстродействия и произвольности выбора.

При представлении открытого текста используется вероятностный метод, поскольку не известно детерминистического полиномиального алгоритма для выписывания большого числа точек произвольной эллиптической кривой над простым конечным полем, поэтому используем вероятностный алгоритм с малой вероятностью неудачи. Порождать случайные точки на E недостаточно: чтобы закодировать большое число возможных сообщений m, необходим какой-то систематический способ порождения точек, которые были бы связаны с m определенным образом, например, чтобы x-координата имела с m простую связь. Эта зависимость соблюдается в выбранном методе.

Во всех применяемых алгоритмах будем использовать ассиметричные системы шифрования, что позволит получить дополнительную защиту протокола.

3. Проверка устойчивости протокола к атакам средствами AVISPA

Для проверки протокола на устойчивость к атакам противника был применен пакет AVISPA, доступный на [7].

Выбор этого продукта обусловлен тем, что AVISPA интегрирует все современные подходы к анализу протоколов, такие как проверка на модели, древовидные автоматы, временная логика. При этом используются разработки, созданные после 2000 года. Специально для него были разработаны версии языков для описания протоколов, позволившие существенно расширить класс изучаемых протоколов, а также интегрировать в единую платформу сразу несколько различных методов [1, 7].

При проверке протокола была составлена программа на языке CAS+, которая описывает сеанс связи построенного протокола. Затем средствами пакета SPAN программа переведена в формализованный язык описания протоколов HLPSL, а затем в более низкоуровневый язык IF, по которому уже стало возможным получить результаты проверки устойчивости протокола к атакам средствами AVISPA.

В результате проверки протокола известных атак на протокол не найдено. Злоумышленник может получить доступ к информации, только решив задачу дискретного логарифмиро-

вания на эллиптической кривой. Знания злоумышленника после сеанса протокола показаны на рис. 1.

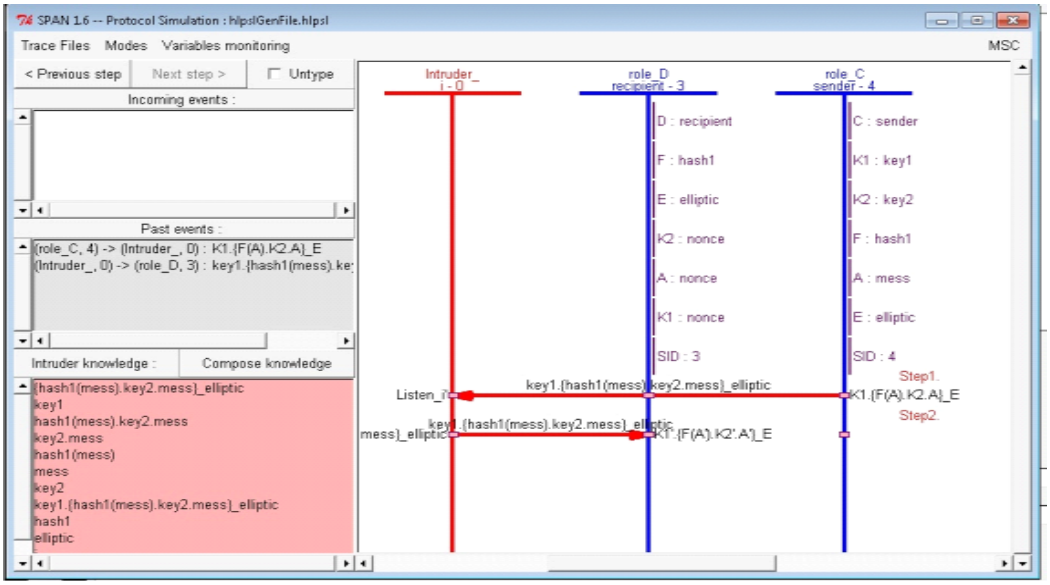

Рис. 1. Результат проверки протокола средствами AVISPA. Злоумышленник (Intruder) и его знания показаны внизу слева

4. Анализ стойкости криптографического протокола на основе эллиптических кривых

Проведение криптоанализа для давно существующих и недавно появившихся криптоалгоритмов очень актуально, так как вовремя можно сказать, что данный криптоалгоритм нестоек, и усовершенствовать его или заменить новым.

Надежность цифровой подписи определяется стойкостью к криптоаналитическим атакам двух ее компонент: хэш-функции и самого алгоритма ЭЦП [8]. В протоколе мы использовали хэш-функцию Tiger. Атака на Tiger-24 (24-х раундовая версия) дает почти псевдоколлизию со сложность 2^{47} операций до взлома, при этом используется 192-битное хэш-значение [6].

Стойкость алгоритма цифровой подписи для построенного протокола определяется стойкостью цифровой подписи Шнорра и шифрованием по системе Эль-Гамаля на эллиптических кривых.

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, вычислительная сложность которого оценивается как O(exp(c(ln p)1/3(ln ln q)2/3)) операций в поле Fq, где c=1,92 [8]. При характеристике поля порядка 160 двоичных разрядов (бит) стойкость составляет $1,8 \cdot 10^{11}$ операций до взлома.

Стойкость шифрования по системе Эль-Гамаля на эллиптических кривых основана на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой. В настоящее время наиболее быстрыми алгоритмами решения задачи дискретного логарифмирования в группе точек эллиптической кривой при правильном выборе парамет-

ров считаются r-метод и l-метод Полларда [9]. Так, для улучшенного r-метода Полларда вычислительная сложность оценивается как . При характеристике поля порядка 160 бит стойкость составляет $1,94 \cdot 10^{26}$ операций до взлома.

Для обеспечения необходимого уровня стойкости построенного протокола должно выполняться ограничение на характеристику поля: она должна быть более 160 бит [2, 9]. Примечательно, что 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 $5 \cdot 10^{51}$ операций до взлома. Для сравнения, стойкость самого близкого по применяемым идеям и алгоритмам криптографического протокола цифровой подписи, российского стандарта ГОСТ Р 34.10-2001, при использовании аналогичной характеристики поля (160 бит) составляет $1,93 \cdot 10^{35}$ операций до взлома. В настоящее время применяется схема ЭЦП ГОСТ Р 34.10-2001 с характеристикой поля 256 двоичных разрядов, ее стойкость составляет $3,02 \cdot 10^{38}$ операций до взлома [10]. График зависимости стойкости нашего протокола от нижней границы характеристики поля, начиная с 160 бит, приведен на рис. 2.

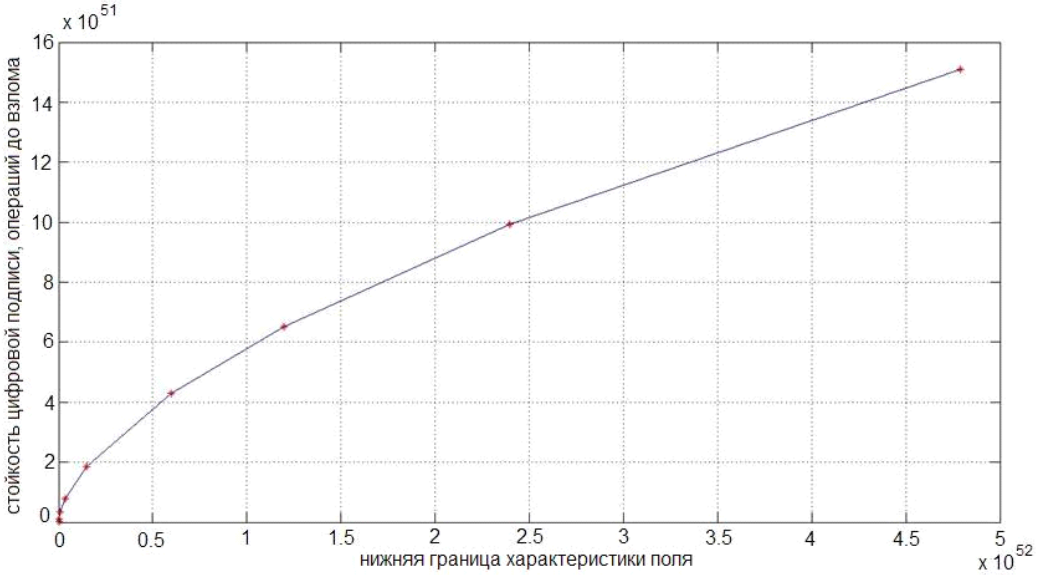

Рис. 2. Зависимость стойкости протокола цифровой подписи от нижней границы характеристики поля

Литература

1. The GNU Multiple Precision Arithmetic Library. – URL: http://gmplib.org (дата обращения: 7.09.2013).
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. Kelsey, J. Collisions and Near-Collisions for Reduced-Round Tiger, Proceedings of Fast Software Encryption / J. Kelsey, S. Lucks. – Graz: FSE, 2006.
5. Tiger: a Fast New Cryptographic Hash Function (Designed in 1995). – URL: http://www.cs.technion.ac.il/ biham/Reports/Tiger (дата обращения: 7.09.2013).

6. Mendel, F. Cryptanalysis of the Tiger Hash Function / F. Mendel, V. Rijmen. – Springer Berlin; Heidelberg: ASIACRYPT, 2007.
7. AVISPA – URL: http://www.avispa-project.org (дата обращения: 7.09.2013).
8. Алгоритмические основы эллиптической криптографии / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М: МЭИ, 2000.
9. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А.Тимофеев, В.Ф. Шаньгин – М.: Радио и связь, 2001.
10. 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 и др. // Радиотехника. – 2000. – № 114. – С. 15–24.

Сергей Геннадьевич Чеканов, кандидат физико-математических наук, доцент кафедры «Алгебра, геометрия и анализ», Дальневосточный федеральный университет (г. Владивосток, Российская Федерация), stepltd@mail.ru.

Bulletin of the South Ural State University.
Series «Mathematical Modelling, Programming & Computer Software»,
2013, vol. 6, no. 2, pp. 120–127.

MSC 11T71

Development, Implementation and Analysis of Cryptographic Protocol for Digital Signatures Based on Elliptic Curves

S.G. Chekanov, Far East Federal University, Vladivostok, Russian Federation, stepltd@mail.ru

Cryptographic primitives based on elliptic curves have become very popular recently. The main reason is that elliptic curves can build many examples of finite Abelian groups with good parameters suitable for cryptographic purposes. In addition, elliptical curves are easy to implement on a computer, and the cryptographic strength can be achieved by choosing the characteristics of the finite field. Software cryptographic protocol for digital signature based on elliptic curves is designed and implemented. The protocol encrypts messages, forming a digital signature, message transmission and decoding at the receiver. Resistant cryptographic protocol is analyzed by several methods. A diagram of dependence of cryptographic security of the protocol on finite field characteristic, over which the elliptic curve is built, is given in the paper. The program in C++ programming environment Visual C++ 2010 with the support of large numbers GMP library is written. The program allows you to encrypt and decrypt the messages according to the generated protocol. It is also the instrument for transmission and receiving the messages with high degree of cryptographic strength and at reasonable rate.

Keywords: cryptography, cryptographic protocols, elliptic curves, the cryptographic strength.

References

1. Cheremushkin A.V. *Kriptograficheskie protokoly: osnovnye svoystva i uyazvimosti* [Cryptographic Protocols: Basic Properties and Vulnerability]. Moscow, Akademiya, 2009.
2. Kobliz N. *Kurs teorii chisel i kriptografii* [The Course of Number Theory and Cryptography]. Moscow, TVP, 2001.

3. Kelsey J., Lucks S. *Collisions and Near-Collisions for Reduced-Round Tiger, Proceedings of Fast Software Encryption.* Graz, FSE, 2006.

4. Mendel F., Rijmen V. *Cryptanalysis of the Tiger Hash Function.* Heidelberg: ASIACRYPT, Springer Berlin, 2007.

5. Bolotov A.A., Gashkov S.B., Frolov A.B., Chasovskikh A.A. *Algoritmicheskie osnovy ellipticheskoy kriptografii* [Algorithmic Foundations of Elliptic Cryptography]. Moscow, MEI, 2000.

6. Romanets U.V., Nimofeev P.A., Shangin V.F. *Zashchita informatsii v komp'yuternykh sistemakh i setyakh* [The Protection of Information in Computer Systems and Networks]. Moscow, Radio i Svyaz', 2001.

7. Bondarenko M.F., Gorbenko I.D., Kachko E.G. Sushchnost' i rezul'taty issledovaniy svoystv perspektivnykh standartov tsifrovoy podpisi X9.62-1998 i raspredeleniya klyuchey X9.63-199X na ellipticheskikh krivykh [The Essence and Results of Research of the Properties of Perspective Digital Signature Standard X9.62-1998 and Key Distribution X9.63-199X on Elliptic Curves]. *Radiotekhnika* [Radiotechnique], 2000, no. 114, pp. 15–24.

Поступила в редакцию 7 сентября 2012 г.