УДК 003.26; 004.056.55

Д.С. Будчан

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Протокол отрицаемого шифрования на основе решения кубических уравнений

В настоящее время особое внимание уделяется проблемам, связанным с безопасностью данных. Защита информации достигается путём применения различных алгоритмов шифрования. Важным критерием алгоритмов является криптостойкость алгоритма. Одним из современных способов шифрования, обеспечивающий высокую крптостойкость, является отрицаемое шифрование. Для повышения криптостойкости протоколов было предложено модифицировать существующий алгоритм решения кубических уравнений в простом конечном поле путём перехода в конечное поле характеристики два. В данной работе приведён сравнительный анализ аналогов и обоснованы преимущества предложенного алгоритма. Дальнейшее развитие темы заключается в разработке алгоритма решения кубических уравнений в конечном бинарном поле и реализации протокола отрицаемого шифрования.

Криптография, шифрование, отрицаемое шифрование, кубическое уравнение, конечное поле характеристики два

Протоколы шифрования используются во многих сферах, в частности новый вид шифрования - отрицаемое шифрование (ОШ) - используется в различных областях [1]. Так протокол отрицаемого шифрования лежит в основе ряда средств компьютерной безопасности, например, Best Crypt (коммерческое приложение по шифрованию дисков для Windows), True Crypt (приложение для Windows, MAC OS и Linux, с возможностью шифрования дисков), StegFS (криптографическая файловая система для Linux с возможностью отказа), Off-the-Record Messaging (криптографический протокол для систем мгновенного обмена сообщениями). Предложенный алгоритм позволит повысить криптостойкость имеющихся протоколов шифрования [2].

Ранее был предложен способ отрицаемого шифрования основанный на генерации и решении кубических уравнений. В работе [3] описан подробный алгоритм генерации коэффициентов уравнения и решения полученного многочлена в простом конечном поле. Данный алгоритм позволил решить важную проблему разработанных ранее алгоритмов отрицаемого шифрования, а именно обеспечил однозначность процедуры дешифрации.

Следующим этапом стало исследование криптостойкости разработанного алгоритма. Следовательно особую значимость приобрела следующая проблема: криптостойкость протоколов отрицаемого шифрования. Объектом исследования является протокол отрицаемого шифрования, основанный на решении кубических уравнений в бинарном конечном поле, а предметом исследования - криптостойкость алгоритма отрицаемого шифрования, основанного на решении кубических уравнений в бинарном конечном поле.

Таким образом, целью работы является разработка протокола отрицаемого шифрования с повышенной криптостойкостью засчёт использования алгоритма решения кубических уравнений в бинарном конечном поле. Для достижения поставленной цели необходимо решить ряд задач, а именно разработать алгоритм решения кубических уравнений в бинарном конечном поле, затем разработать протокол отрицаемого шифрования на основе алгоритма решения кубических уравнений в бинарном конечном поле.

Информационная безопасность включает в себя обеспечение конфиденциальности, целостности и доступности информации. Всё это достигается применением различных алгоритмов шифрования исходных данных. Существуют различные методы шифрования: симметричные и асимметричные, блочные и потоковые. Одним из новых способов криптографического преобразования является отрицаемое шифрование, в котором зашифровываются совместно от двух и более различных сообщений на нескольких различных ключах. Далее представлено описание нескольких способов отрицаемого шифрования.

Одним из распространённых способов отрицаемого шифрования является протокол ОШ на основе стандартной инфрастурктуры открытых ключей. Протокол основан на вычислительной неотличимости шифртекста порождаемого алгоритмом вероятностного шифрования от шифртекста порождаемого алгоритмом отрицаемого шифрования. Предложенный протокол не использует общие секретные ключи, является стойким к двусторонним принуждающим атакам и активным принуждающим атакам, когда злоумышленник выдаёт себя за легального участника протокола.

Следующим аналогом является протокол ОШ, основанный на решении кубических уравнений в простом конечном поле. Особенность алгоритма заключается в однозначности процесса дешифрации, которая достигается засчёт генерации кубического уравнения, имеющего единственный корень. Подробнее протокол описан в работах [4, 5].

Для сравнения алгоритмов имеет смысл привести некоторый иной протокол, например, распространённый протокол AES. AES не относится к протоколом отрицаемого шифрования. Advanced Encryption Standard — симметричный алгоритм блочного шифрования, принятый в качестве стандарта шифрования правительством США [6]. Этот алгоритм хорошо проанализирован и сейчас широко используется. В 2002 году AES был объявлен стандартом шифрования. Стандарт определяется публикацией FIPS 197 и используется в разнообразных приложениях, где предъявляются повышенные требования к производительности и безопасности, также обладает достаточно высокой криптостойкостью.

Рассмотрены следующие критерии, на основе которых проведено сравнение ряда алгоритмов шифрования данных.

Одним из критериев является сложность реализации. Данный критерий может влиять на стоимость разработки и поддержки протокола, так как в зависимости от сложности требуется, например, работа более квалифицированного сотрудника.

Следующим рассмотрен критерий, связанный со скоростью работы алгоритма. В настоящее время критерий не имеет такой важности, как ранее, ввиду увеличения вычислительной мощности устройств, однако для общего сравнения предложенных аналогов данный критерий будет включён, так как при прочих равных данный критерий может оказаться решабщим при выборе алгоритма шифрования.

Одним из крайне значительных критерийев является криптостойкость. Важный критерий, на основе которого производится выбор того или иного протокола шифрования. Отвечает за одну из задач шифрования - обеспечение конфиденциальности информации, то есть невозможности прочтения информации посторонним. Стойким считается такой алгоритм, успешная атака на который требует от атакующего обладания недостижимым на практике объёмом вычислительных ресурсов или перехваченных открытых и зашифрованных сообщений либо настолько значительных затрат времени на расшифровку, что к моменту получения искомых данных защищённая информация утратит свою актуальность [7]. В большинстве случаев криптостойкость не может быть математически доказана: в случае отрицаемого шифрования на основе решения уравнений можно свести задачу взлома алгоритма к задаче нахождения корней кубического уравнения в бинарном конечном поле, которая считается вычислительно сложной (в результате можно показать, что взлом не легче решения этой задачи).

В таблице 1 приведены перечисленные способы шифрования и критерий, на основе которых можно провести обобщённое сравнение существующих аналогов.

Таблица 1

Аналог	Сложность реализации	Скорость	Криптостойкость
ОШ + стандартная инфраструктура	-	+	-
ОШ + куб.ур в простом поле	+	+	+
Иной протокол (пр-р: AES)	-	+	+
ОШ + куб.ур. в бин-ом поле	+	+	++

В результате сравнения можно сделать вывод, что предложенный алгоритм имеет преимущества по сравнению с существующими аналогами, а следовательно разработка алгоритма актуальна и обоснована. Несмотря на более сложную реализацию, предложенный лагоритм не уступает аналогам в скорости и имеет преимущество в криптостойкости, что является особым достоинством.

В результате изучения и анализа существующих алгоритмов шифрования можно сделать вывод, что для повышения криптостойкости необходима разработка и реализация протоколов отрицаемого шифрования. Отрицаемое шифрование значительно превосходит стандартные алгоритмы в защите от

принуждающих атак [2]. Таким образом можно сделать вывод, что в общем виде искомое решение должно обладать свойством отрицаемости. В настоящее время существует ряд протоколов отрицаемого шифрования. Высокой криптостойкостью обладают протоколы, основанные на генерации и решений уравнений различной степени. Однако некоторые из имеющихся алгоритмов не обладают однозначностью решения, что делает такие протоколы непригодными для использования. Поэтому важным критерием разрабатываемого алгоритма является существование и единственность решения уравнения. Один из предложенных для сравнения алгоритмов обладает свойством однозначности решения (алгоритм решения кубических уравнений в простом конечном поле). Следующим этапом является модификация данного алгоритма и повышение криптостойкости основанного на нём протокола. Таким образом получили следующие характеристики, которыми должен обладать разрабатываемый алгоритм: - свойство отрицаемости (повышение устойчивости к принуждающим атакам); - существование и единственность решения уравнения, лежащего в основе протокола; - повышенная криптостойкость (в данном случае за счёт перехода из простого конечного поля в бинарное).

Протокол отрицаемого шифрования, основанный на алгоритме генерации и решения кубического уравнения, состоит из нескольких этапов. Этапы являются шагами общей схемы симметричного шифроавния, применяемой во многих протоколах шифрования [8]. В качестве основных частей можно выделить генерацию шифротекста в виде коэффициентов уравнения, передача шифротекста получателю, решение уравнения, составленного из коэффициентов, входящих в полученный шифротекст. Для описания алгоритма необходимо определить значения открытого и закрытого ключей, что будет сделано в дальнейшем. Основываясь на разработанном ранее алгоритме решения кубических уравнений в простом конечном поле, можно предположить, что основные характеристики открытого и секретного ключей будут связаны с сильными простыми числами. Одним из важным требований, предъявляемых к алгоритму, является однозначность получаемого после дешифрации результата, то есть наличие единственного корня у решаемого кубического уравнения. Для того чтобы процесс имел однозначное расшифровывание, необходимо чтобы кубическое уравнение имело единственный корень в результате его решения. Для этого необходимо разложить уравнение на два множителя, один из которых является квадратным уравнением.

$$x^3+Ax^2+Bx+D=(x-M)(x^2+Zx+Y) \quad (1)$$

При условии, что данное квадратное уравнение не будет иметь корней, получим кубическое уравнение, имеющие единственный корень, что позволит добиться однозначности процесса дешифрации. После того, как будут определены открытый и закрытый ключи и указаны требования к исходным значениям, можно переходить к описанию алгоритма шифрования сообщения, который заключается в генерации коэффициентов уравнения.

Для этого по аналогии с имеющимися способами отрицаемого шифрования выполняется одновременное зашифрование двух сообщений — фиктивного $M < n$ и секретного $T < n$. При этом фиктивное сообщение M шифруется по открытому ключу, а секретное сообщение зашифровывается по формуле (2):

$$Z(T) \bmod n, \quad (2)$$

т. е. секретное сообщение встраивается в число Z, которое используется в качестве случайного значения в алгоритме открытого шифрования (является одним из коэффициентов квадратного уравнения (1). Полученная в результате процесса шифрования криптограмма $C = (A, B, D)$ отправляется владельцу открытого ключа по открытому каналу. Получатель расшифровывает её с помощью личного закрытого ключа, получая фиктивное сообщение M. Для расшифровки истинного секретного сообщения понадобится дополнительный шаг вычислений, основанный на применении дополнительного истинного секретного ключа. Необходимо поделить многочлен x^3+Ax^2+Bx+D на двучлен $(x - M)$, в результате чего будет получен трехчлен x^2+Zx+Y и будет вычислено секретное сообщение по формуле, обратной (2). Пошаговая процедура расшифровывания будет составлена на основе алгоритма генерации уравнения.

Перечисленные алгоритмы генерации кубического уравнения и его решения, процедуры генерации открытого и закрытого ключей, а также алгоритм шифрования сообщения могут быть использованы в протоколе отрицаемого шифрования. Главная особенность протокола заключается в стойкости к принудительным атакам на отправителя сообщения.

В случае принуждения отправителя сообщения к раскрытию использованных параметров шифрования он предоставляет атакующему фиктивное сообщение M и число Z, ссылаясь на последнее как на случайное

значение. Выполнив шифрование M по открытому ключу при использовании предоставленного "случайного" значения Z, атакующий получит криптограмму $C = (A, B, D)$. Если она совпадает с шифртекстом, переданным по открытому каналу и который по предположению известен атакующему, то последний вынужден признать, что ему честно раскрыли переданное сообщение. Чтобы раскрыть обман атакующему, нужно восстановить секретное сообщение по известному значению Z, однако это требует значительных вычислительных затрат, что не менее сложно, чем решение задачи факторизации числа n [9]. Таким образом будет обеспечено свойство отрицаемости, а именно в случае принуждающей атаки будет возможность раскрыть атакующему фиктивный ключ, с помощью которого будет расшифровано фиктивное сообщение, при этом истинное сообщение останется скрытым.

В данной статье предложен способ отрицаемого шифрования, основанный на алгоритме генерации и решения кубического уравнения в конечном поле характеристики два. Выделены критерии оценки различных способов шифрования, а также проведено описание ряда аналогов. На основе критериев сделаны выводы о преимуществах предложенного способа по сравнению с существующими аналогами, а именно ожидается повышенная криптостойкость алгоритма за счёт перехода в бинарное конечное поле. Таким образом разработка описанного алгоритма позволит достигнуть поставленной цели – повышения криптостойкости алгоритма отрицаемого шифрования. В дальнейшем необходимо разработать алгоритм генерации коэффициентов уравения и на основе алгоритм генерации и решения кубического уравнения в бинарном конечном поле разработать протокол отрицаемого шифрования.

Список литературы

1. Meng B., Wang J-Q. A Receiver Deniable Encryption Scheme // Proceedings of the 2009 International Symposium on Information Processing (ISIP'09) - Huangshan, P. R. China, August 21-23, 2009. P. 254-257.
2. Canetti R., Dwork C., Naor M., Ostrovsky R. Deniable encryption // Annual International Cryptology Conference - Springer, Berlin, Heidelberg. P. 90-104.
3. Будчан Д.С. Разработка алгоритма решения кубических уравнений в конечном поле и реализация протокола отрицаемого шифрования / ВКР, СПбГЭТУ "ЛЭТИ", 2016 - 54 с.
4. Молдовян, Н. А. Генерация кубических уравнений как способ открытого шифрования / Н. А. Молдовян, Д. Н. Молдовян, М. А. Вайчикаускас // Вопросы защиты информации. — 2015. — Выпуск 2. — С. 3—7.
5. Молдовян Н. А., Вайчикаускас М. А. Расширение криптосхемы Рабина: алгоритм отрицаемого шифрования по открытому ключу // Вопросы защиты информации. 2014. № 2. С. 12—16.
6. Announcing the Advanced Encryption Standard (AES) // Federal Information, Processing Standards Publication 197. November 26, 2001.
7. Адигеев М.Г. Введение в криптографию // Ростовский государственный университет. 2002.
8. Ayushi. A Symmetric Key Cryptographic Algorithm // International Journal of Computer Applications (0975 - 8887). 2010. Vol. 1. P/ 352-355.
9. Moldovyan N. A., Moldovyan A. A. Class of Provably Secure Information Authentication Systems // Springer Verlag CCIS. 2007. Vol. 1. P.147–152 / 4th Int. Workshop MMM-ANCS'07 Proc. September 13—15, 2007.

D.S. Budchan

Saint Petersburg Electrotechnical University "LETI"

The Deniable Encryption Protocol based on the solution of cubic equations

Currently, special attention is paid to problems related to data security. Information security is achieved through the use of various encryption algorithms. An important criterion of algorithms is the cryptostability of the algorithm. One of the modern methods of encryption, which provides high creep resistance, is deniable encryption. To increase the cryptographic strength of the protocols, it was suggested to modify the existing algorithm for solving cubic equations in a simple finite field by passing to the final field of characteristic two. In this paper, a comparative analysis of analogues and substantiate the advantages of the proposed algorithm is presented. Further development of the topic consists in developing an algorithm for solving cubic equations in a finite binary field and implementing a protocol of deniable encryption.

Cryptography, encryption, deniable encryption, cubic equation, binary finite field