УДК 681.3

КОММУТАТИВНЫЕ ШИФРЫ НА ОСНОВЕ ТРУДНОСТИ ОДНОВРЕМЕННОГО РЕШЕНИЯ ЗАДАЧ ФАКТОРИЗАЦИИ И ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ

А. А. Молдовян[а], *доктор техн. наук, начальник научно-исследовательского отдела проблем информационной безопасности, профессор*
А. Н. Березин[б], *аспирант*
А. В. Рыжков[б], *аспирант*
[а]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*
[б]*Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Санкт-Петербург, РФ*

Постановка проблемы: *известны построения криптосхем с открытым ключом, при которых их взлом требует одновременного решения двух независимых вычислительно трудных задач, за счет чего обеспечивается повышение уровня их безопасности, однако аналогичные построения для алгоритмов коммутативного шифрования не известны. Практическая значимость задачи повышения безопасности используемых криптографических механизмов защиты информации обусловливает актуальность проблемы уменьшения вероятности взлома алгоритмов коммутативного шифрования за счет появления прорывных результатов в области решения вычислительно трудных задач. Целью работы является разработка алгоритмов коммутативного шифрования, взлом которых требует одновременного решения двух независимых вычислительно трудных задач.* ***Методы:*** *расщепление шифруемых сообщений и использование разовых ключей шифрования.* ***Результаты:*** *впервые предложен метод расщепления сообщений для расширения класса вычислительно трудных задач, которые могут быть положены в основу коммутативных шифров, разработан алгоритм коммутативного шифрования, основанный на трудности задачи факторизации, а также алгоритм коммутативного шифрования, стойкость которого основана на вычислительной трудности одновременного решения задач факторизации и задачи дискретного логарифмирования в конечном поле. Сформулированы необходимые требования к выбору параметров для предложенных алгоритмов.* ***Практическая значимость:*** *существенное повышение уровня безопасности процедуры коммутативного шифрования.*

Ключевые слова *— компьютерная безопасность, криптография, коммутативное шифрование, задача факторизации, задача дискретного логарифмирования.*

Введение

Коммутативное шифрование применяется для решения ряда специфических задач, таких как электронная жеребьевка, протоколы бесключевого шифрования и игра в покер по телефону [1]. Самым известным представителем алгоритмов коммутативного шифрования (АКШ) является алгоритм Полига — Хеллмана [2]. Для повышения производительности процедур коммутативного шифрования в работе [3] была предложена его реализация над конечным расширенным полем, заданным в явной векторной форме. Это достигается благодаря сравнительно низкой сложности операции умножения и возможности эффективного распараллеливания в полях указанного типа.

Относительно безопасности криптосхем ранее [4] было предложено рассматривать понятие безопасности как характеристику, учитывающую стойкость W криптографических механизмов и вероятность P появления в обозримом будущем эффективных способов их взлома, основанных на прорывных достижениях в области решения вычислительно трудных задач. Таким образом, отношение W/P вводится как некоторый интегральный параметр безопасности. Снижение указанной вероятности может быть достигнуто разработкой криптосхем, взлом которых требует одновременного решения двух независимых трудных задач. В подобных криптосхемах вероятность взлома равна произведению малых вероятностей появления прорывного решения каждой из указанных двух задач, благодаря чему вероятность взлома криптосхем заметно снижается, что означает существенное повышение их безопасности.

В данной статье предлагается механизм расщепления сообщений, позволяющий снять ограничения на шифруемые сообщения при использовании вычислительной трудности задачи факторизации (ЗФ), и АКШ, основанный на трудности одновременного решения ЗФ и задачи дискретного логарифмирования (ЗДЛ), обеспечивающий более высокий уровень безопасности.

Особенности использования задачи факторизации в коммутативных шифрах

Механизм коммутативного шифрования работает следующим образом. Для всех сообщений, значения которых выражаются числами $\alpha^i \bmod n$, где $i = 1, 2, ..., \gamma$, используя известное значение γ, каждый пользователь генерирует случайное значение $e < \gamma$ и вычисляет $d = e^{-1} \bmod \gamma$. Пара значений e и d составляет ключ зашифрования и расшифрования соответственно. Отметим, что в от-

личие от схем шифрования с открытым ключом, значения обоих ключей держатся в секрете. При этом шифрование обладает свойством коммутативности, что позволяет зашифровывать и расшифровывать сообщение на различных ключах в различном порядке.

В случае построения АКШ с использованием вычислений по трудно разложимому модулю n, представляющему собой произведение двух больших сильных простых чисел r и q ($n = rq$) [5], вычисления по различным модулям не обладают свойством коммутативности. Следовательно, значение составного модуля не может быть секретным, как в схеме Полига — Хеллмана [2], и должно быть общесистемным параметром, т. е. должно быть известно всем пользователям, поскольку предполагается, что если стойкость алгоритма основывается на ЗФ, то значение n должно вырабатываться некоторым доверительным центром, который уничтожит сгенерированные им сильные простые числа r и q после вычисления значения модуля. Из-за этого для пользователей становится вычислительно невыполнимым нахождение функции Эйлера $\varphi(n) = (r - 1)(q - 1)$ от модуля, что является необходимым условием для генерации пары значений e и d таких, что $ed = 1 \bmod \varphi(n)$. Наличие такой пары значений позволяет построить АКШ. Однако знание значения $\varphi(n)$, которое могло бы предоставляться пользователям доверительным центром, позволит легко факторизовать модуль методом, описанным в работе [1]. Если значения e и d будут генерироваться доверительным центром, то два различных пользователя могут обменяться своими секретными значениями и найти r и q, т. е. взломать такую систему коммутативного шифрования [1].

В качестве механизма, использующего известные параметры, зависящие от множителей модуля n, который не позволит пользователям использовать вышеописанные атаки, можно применить следующую схему [6] формирования числа α, порядок которого равен достаточно большому простому числу γ.

Генерируются простые r и q такие, что достаточно большое простое γ делит оба числа $r - 1$ и $q - 1$. Число, имеющее порядок γ по модулю n, выбирается в качестве α. В этом случае значение γ будет несекретным.

Данные условия позволяют сохранить высокую трудность ЗФ модуля n при известных значениях α, n и γ [4]. При этом обеспечение практической невозможности факторизации модуля n задается тем, что значения n, α и γ генерируются некоторым доверительным центром.

Отметим, что процедуры АКШ корректно работают только для тех сообщений, которые представимы в виде значений $\alpha^i \bmod n$. При практическом применении требуется выполнять шифрование самых различных сообщений, в том числе и случайных битовых строк, которые могут быть не представимы в виде степени числа α, т. е. не все сообщения можно зашифровать данным способом. Схожая проблема имеется и при разработке АКШ с использованием эллиптических кривых (ЭК), заданных над конечными полями. Причиной этому служит то, что координаты ЭК должны удовлетворять некоторому уравнению третьей степени. Это значит, что не все пары значений соответствуют точкам ЭК. Легко видеть, что построение АКШ в обоих случаях требует решения задачи кодирования сообщений либо точками ЭК, либо значениями из некоторого ограниченного множества. Подходы к решению данной задачи не очевидны.

В частных случаях приложений коммутативных шифров требуется зашифровать сравнительно небольшое число заранее известных сообщений (например, в протоколе игры в покер по телефону). В этих случаях можно закодировать известные сообщения значениями вида $\alpha^i \bmod n$. Однако для построения АКШ случайных сообщений, основанного на трудности ЗФ, данный подход не применим непосредственно. Для того чтобы с помощью предлагаемого механизма можно было выполнить коммутативное шифрование произвольных сообщений, требуется использовать дополнительный механизм расщепления сообщений, который описан далее.

Механизм расщепления сообщений

Число значений вида $\alpha^i \bmod n$ равно $\gamma \geq 2^{160}$ для обеспечения 80-битовой стойкости (т. е. стойкости, равной 2^{80} операций модульного умножения). Эти значения практически невозможно перебрать, поэтому их можно использовать в качестве ключа шифрования. Пусть требуется зашифровать сообщение $|M| < n$. Сгенерируем случайное число $k < \gamma$ и вычислим значение $K = \alpha^k \bmod n$. Зашифруем сообщение M в зависимости от K по модулю n, например, по достаточно простой формуле $C = (M + K)K \bmod n$, которая обеспечивает возможность безопасного шифрования коротких сообщений. Более простые формулы $C = M + K \bmod n$ и $C = MK \bmod n$ допускают раскрытие коротких сообщений или сообщений из заранее известного ограниченного набора $\{M_1, M_2, ..., M_i, ...\}$, используя в качестве критерия распознавания истинного сообщения равенство порядка значений $K_i = C - M_i$ и $K_i = CM_i^{-1} \pmod n$ соответственно числу γ (т. е. проверяя выполнимость соотношения $K_i = 1 \bmod n$). Сообщение M легко восстанавливается из пары значений (C, K), поэтому можно говорить о расщеплении сообщения M на два значения C и K, причем C — число произвольного вида, а число K принадлежит

множеству значений $\{\alpha^1 \bmod n, \alpha^2 \bmod n, ..., \alpha^\gamma \bmod n\}$. После расщепления сообщения M его зашифрование (расшифрование) можно выполнить как зашифрование (расшифрование) значения K. Последнее можно выполнить путем возведения K в степень e по модулю n по формуле $S = K^e \bmod n$. Расшифрование выполняется как возведение криптограммы S в степень d по модулю n, т. е. по формуле $S^d \bmod n = K$. Значение C, по которому можно восстановить сообщение M, не подвергается какому-либо преобразованию в процессе шифрования. Получаем следующую схему коммутативного шифрования (АКШ1).

1. При первичном шифровании сообщения M выполняется его расщепление, т. е. представление сообщения в виде $M = (C, K)$, и шифрование значения K: $S = K^e \bmod n$. На выходе первичной процедуры шифрования имеем пару значений (C, S).

2. Последующие шаги зашифрования (расшифрования) выполняются над значением S.

3. Завершающий шаг расшифрования выполняется как расшифрование значения S, приводящее к восстановлению значения K, выбранного на шаге первичного шифрования сообщения, и вычисление значения M по формуле $M = CK^{-1} - K \bmod n$.

Данный АКШ позволяет выполнить шифрование сообщений $M < n$ произвольного вида за счет применения механизма расщепления шифруемого сообщения — представления сообщения в виде пары других сообщений, одно из которых представляет собой число вида $\alpha^i \bmod n$ при некотором значении $i \in \{1, 2, ..., \gamma\}$. Для его взлома потребуется решить ЗДЛ по составному модулю n, что требует решения ЗФ, ЗДЛ по модулю r и ЗДЛ по модулю q. При выборе числа n ограниченного размера (например, 1024 бит) безопасность данного АКШ определяется только ЗФ, поскольку при таком размере числа n сложность указанных двух вариантов ЗДЛ является достаточно низкой.

Алгоритм коммутативного шифрования, взлом которого требует одновременного решения двух независимых трудных задач

Нетрудно заметить, что алгоритм Полига — Хеллмана может быть естественным образом встроен в описанный ранее АКШ при использовании в первом простого числа $p > n$. Это реализуется путем одновременного шифрования обоих значений, представляющих сообщение M в расщепленном виде. Для этого каждый пользователь выбирает две пары ключей (e_1, d_1) и (e_2, d_2), удовлетворяющих условиям $e_1 d_1 = 1 \bmod \gamma$ и $e_2 d_2 = 1 \bmod p - 1$. Шифрование первого значения в паре расщепления выполняется по первой паре подключей как возведение в степень e_1 (зашифрование) или d_1 (расшифрование) по модулю p. Шифрование второго значения в паре расщепления выполняется по второй паре подключей как возведение в степень e_2 (зашифрование) или d_2 (расшифрование) по модулю n. Получаем следующую схему коммутативного шифрования (АКШ2).

1. Первичное зашифрование сообщения M выполняется как представление M в виде $M = (C, K)$, зашифрование C по формуле $C^* = C^{e_1} \bmod p$ и зашифрование K по формуле $S = K^{e_2} \bmod n$. На выходе первичной процедуры шифрования имеем пару значений (C^*, S).

2. Последующие шаги зашифрования (расшифрования) выполняются как шифрование значения S путем выполнения операции возведения в степень e_2 по модулю n и шифрование значения C^* путем выполнения операции возведения в степень e_1 по модулю p.

3. Завершающий шаг расшифрования выполняется как расшифрование значения S, приводящее к восстановлению значения K; расшифрование значения C^*, приводящее к восстановлению значения C, и вычисление значения M по формуле $M = CK^{-1} - K \bmod n$.

Нетрудно видеть, что взлом данного АКШ требует одновременного решения ЗФ и ЗДЛ в конечном простом поле. Шифрование второго элемента пары расщепления осуществляется как возведение в секретную степень по модулю n, поэтому можно говорить не о ЗФ, а о ЗДЛ по трудно разложимому модулю n. Причем последняя задача принципиально отличается от ЗДЛ по простому модулю. В частности, алгоритм решения ЗДЛ по модулю n может быть использован для факторизации значения модуля n [7], что показывает существенную связь ЗФ и ЗДЛ по составному модулю n [5].

Использование задачи дискретного логарифмирования по составному модулю

В работах [4, 7, 8] предложено использовать связь ЗФ и ЗДЛ по составному модулю n. Если вычислительная сложность решения ЗФ и ЗДЛ (при использовании лучших известных алгоритмов решения этих задач) больше необходимого уровня стойкости, то взлом криптосхем, основанных на сложности решения ЗДЛ по составному модулю, потребует одновременного решения двух трудных задач ЗФ и ЗДЛ. Таким образом, выбор достаточно больших размеров простых делителей r и q числа n в алгоритме, описанном в предыдущем разделе, превращает последний в АКШ (АКШ3), основанный на трудности одновременного решения ЗФ и ЗДЛ по простому модулю, т. е. без дополнительного использования алгоритма Полига — Хеллмана.

Задача дискретного логарифмирования по составному модулю n ($y = \alpha^x \bmod n$) может быть реше-

■ Сравнение предложенных АКШ с АКШ Полига — Хеллмана

Показатель	АКШ Полига — Хеллмана	АКШ1	АКШ2	АКШ3
Трудная задача, решение которой требуется для взлома алгоритма	ЗДЛ	ЗФ	ЗДЛ+ЗФ	ЗДЛ+ЗФ
Отношение размера криптограммы к размеру исходного текста	1	2	2	2
Количество операций возведения в степень, выполняемых при зашифровании (расшифровании) сообщения	1 (1)	1 (1)	2 (2)	1 (1)
Размеры параметров для обеспечения 80-битовой стойкости (битовый размер числа x обозначен как $\|x\|$)	$\|p\| \geq 1024$ бит $\|e\| \leq \|p-1\|$ $\|d\| \approx \|p-1\|$	$\|p\| \geq 1024$ бит $\|n\| \geq 1024$ бит $\|\gamma\| \geq 160$ бит $\|e_1\|, \|d_1\| = \|\gamma\|$ $\|e_2\|, \|d_2\| = \|p-1\|$	$\|n\| \geq 1024$ бит $\|\gamma\| \geq 160$ бит $\|e\|, \|d\| = \|\gamma\|$	$\|p\| \geq 1024$ бит $\|q\| \geq 1024$ бит $\|n\| \geq \|pq\|$ $\|\gamma\| \geq 160$ бит $\|e\|, \|d\| = \|\gamma\|$

на путем факторизации модуля n и решения ЗДЛ по множителям r и q [5]:

$$y = a^x \bmod r;\ y = a^x \bmod p.$$

Очевидно, что решение x является одинаковым для обоих уравнений, так как порядок α по модулям r и q одинаков и равен γ. В случае выбора одинаковой длины делителей r и q вычислительная сложность ЗФ модуля n примерно в 2 раза превышает сложность ЗДЛ по простому модулю r или q. Поэтому взлом криптосхемы требует одновременного решения ЗФ и ЗДЛ, если вычислительная сложность решения каждой из этих задач обеспечивает уровень стойкости, превышающий заданный. При этом за стойкость криптосхемы следует принять меньшее из значений трудоемкости решения ЗФ и ЗДЛ. С учетом этого размер минимального из делителей составного числа n должен быть выбран таким, чтобы трудоемкость ЗДЛ по модулю этого делителя соответствовала заданному уровню стойкости, например, 1024 бит при 80-битовой стойкости.

Заключение

Впервые предложены АКШ, основанные на трудности ЗФ (это расширяет арсенал коммутативных шифров), в том числе алгоритмы, стойкость которых основана на трудности одновременного решения ЗФ и ЗДЛ (это значительно повышает интегральный показатель безопасности). Существенным элементом предложенных алгоритмов является механизм расщепления сообщений, который позволяет снять ограничение на шифруемые сообщения, накладываемое ЗФ при ее использовании для построения АКШ и состоящее в том, что сообщения должны иметь значения из циклической подгруппы, генерируемой заданным порождающим элементом. Сравнение предложенных АКШ с базовым алгоритмом Полига — Хеллмана приведено в таблице.

Алгоритмы шифрования, использующие механизм расщепления сообщения, могут быть отнесены к классу вероятностных шифров, так как в них при шифровании используются случайные значения, вследствие чего размер шифртекста превышает размер исходного сообщения. В предложенных алгоритмах шифрования размер зашифрованного текста примерно в 2 раза больше размера шифруемого сообщения. Однако это позволяет построить АКШ на основе трудности одновременного решения ЗФ и ЗДЛ в конечном поле, за счет чего решается задача повышения уровня безопасности процедур коммутативного шифрования.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 14-07-00061-а.

Литература

1. **Молдовян А. А., Молдовян Н. А.** Введение в криптосистемы с открытым ключом. — СПб.: БХВ-Петербург, 2005. — 286 с.
2. **Hellman M. E., Pohlig S. C.** et al. Exponentiation Cryptographic Apparatus and Method. U.S. Patent, no. 4424414, 1984.
3. **Молдовяну П. А., Молдовян Д. Н., Морозова Е. В., Пилькевич С. В.** Повышение производительности

процедур коммутативного шифрования // Вопросы защиты информации. 2009. № 4. С. 24–31.
4. **Березин А. Н., Биричевский А. Р., Молдовян Н. А.** Особенности задачи дискретного логарифмирования по составному модулю как криптографического примитива // Информационная безопасность регионов России (ИБРР–2011): тр. 7-й Междунар. конф., Санкт-Петербург, 26–28 октября 2012 г. СПб., 2012. С. 104–108.
5. **Menezes A. J., Vanstone S. A.** Handbook of Applied Cryptography. — N. W.: CRC Press, 1996. — 750 p. doi:10.1201/9781439821916
6. **Moldovyan A. A., Moldovyan D. N., Gortinskaya L. V.** Cryptoschemes Based on New Signature Formation Mechanism // Computer Science Journal of Moldova. 2006. N 3. P. 397–411.
7. **Berezin A. N., Moldovyan N. A., Shcherbacov V. A.** Cryptoschemes Based on Difficulty of Simultaneous Two Different Difficult Problems // Computer Science Journal of Moldova. 2013. N 2. P. 280–290.
8. **Демьянчук А. А., Молдовян Д. Н., Новикова Е. С., Гурьянов Д. Ю.** Подход к построению криптосхем на основе нескольких вычислительно трудных задач // Информационно-управляющие системы. 2013. № 2. С. 60–66.

UDC 681.3

Commutative Ciphers Based on Difficulty of Simultaneous Solving Factorization and Discrete Logarithm Problems

Moldovyan A. A.[a], Dr. Sc., Tech., Head of a Research Division, Professor, maa1305@yandex.ru
Berezin A. N.[b], Post-Graduate Student, a.n.berezin.ru@gmail.com
Rizhkov A. V.[b], Post-Graduate Student, aryzhk@gmail.com
[a]Saint-Petersburg Institute for Informatics and Automation of RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg State Electrotechnical University «LETI», 5, Professora Popova St., 197376, Saint-Petersburg, Russian Federation

Purpose: There are well-known public-key cryptoscheme designs whose breaking requires a simultaneous solution of two independent computationally hard problems. This makes the cryptoscheme security higher; however, similar designs for commutative encryption algorithms are unknown. The practical significance of improving security of cryptographic mechanisms in information protection makes it vital to look for breakthrough innovations in solving computationally hard problems. This paper deals with developing commutative ciphers whose breaking requires a simultaneous solution of two independent computationally hard problems. **Methods:** Splitting the encrypted messages and using one-pad encryption keys. **Results:** For the first time a message-splitting method was proposed which extends the class of computationally hard problems applicable to commutative encryption design. A new commutative cipher was developed, based on the factoring problem, along with a new commutative cipher based on the difficulty of simultaneously solving both a factoring problem and a discrete logarithm problem in the finite field. The requirements were formulated for the selection of the parameters for the proposed algorithms. **Practical relevance:** Essential improvement was provided for the commutative encryption security.
Keywords — Computer Security, Cryptography, Commutative Encryption, Factorization Problem, Discrete Logarithm.

References

1. Moldovyan A. A., Moldovyan N. A. *Vvedenie v kriptosistemy s otkrytym kliuchom* [Introduction to Public-Key Cryptography]. Saint-Petersburg, BHV-Peterburg Publ., 2005. 286 p. (In Russian).
2. Hellman M. E., Pohlig S. C., et al. *Exponentiation Cryptographic Apparatus and Method*. U.S. Patent, no. 4424414, 1984.
3. Moldovyanu P. A., Moldovyan D. N., Morozova E. V., Pil'kevich S. V. Increasing Performance of the Commutative Encryption Procedures. *Voprosy zashchity informatsii*, 2009, vol. 4, pp. 24–31 (In Russian).
4. Berezin A. N., Birichevskii A. R., Moldovyan N. A. Peculiarities of the Discrete Logarithm Problem Modulo a Composite Number as Cryptographic Primitive. *Trudy 7 Sankt-Peterburgskoi mezhregional'noi konferentsii "Informatsionnaia bezopasnost' regionov Rossii" (IBRR–2011)* [Proc. VII Saint-Petersburg Intern. Conf. "Information Security of Russian Regions" (ISRR-2011)]. Saint-Petersburg, 2012, pp. 104–108 (In Russian).
5. Menezes A. J., Vanstone S. A. *Handbook of Applied Cryptography*. N. W., CRC Press, 1996. 750 p. doi:10.1201/9781439821916
6. Moldovyan A. A., Moldovyan D. N., Gortinskaya L. V. Cryptoschemes Based on New Signature Formation Mechanism. *Computer Science Journal of Moldova*, 2006, vol. 14, no. 3, pp. 397–411.
7. Berezin A. N., Moldovyan N. A., Shcherbacov V. A. Cryptoschemes Based on Difficulty of Simultaneous Two Different Difficult Problems. *Computer Science Journal of Moldova*, 2013, vol. 21, no. 2, pp. 280–290.
8. Dem'ianchuk A. A., Moldovyan D. N., Novikova E. S., Gur'ianov D. Iu. An Approach to Cryptoscheme Design Based on Several Computationally Hard Problems. *Informatsionno-upravliaiushchie sistemy*, 2013, no. 2, pp. 60–66 (In Russian).