Обмен информацией клиентов с УЦ может быть защищен также с помощью симметричного алгоритма защитного кодирования.

Формирование сеансовых ключей – по протоколу Диффи-Хеллмана (DH, ECDH) [1, 5] или его современным обобщениям DHL, DHFL [3, 4, 6, 7].

Литература

1. Шнайер, Б. Прикладная криптография. – Изд. 3-е / Б. Шнайер. – Москва: «Триумф», 2018. – 610 с.

2. Лебедев, Г. А. Новые однонаправленные функции / Г.А. Лебедев // Флеровские чтения : сборник тезисов четвертой школы-конференции молодых исследователей. – ОИЯИ, Дубна, 2011. – С. 5–7,

3. Лебедев Г. А. Применение знаково-цифровых систем счисления для вычисления однонаправленных функций / Г. А. Лебедев // Тезисы «XI Школьные Харитоновские чтения». – РФЯЦ-ВНИИЭФ, Саров, 2011. – С. 16–18.

4. Лебедев, А. Н. Обобщенный протокол Диффи-Хеллмана с аутентификацией сторон / А. Н. Лебедев // Международная алгебраическая конференция, посвященная 110-летию со дня рождения профессора А.Г. Куроша. – М.: Издательство МГУ, 2018. – С. 123–127.

5. Diffie, W. New Directions in Cryptography / W. Diffie, M. E. Hellman // IEEE Trans. Inform. Theory, 1976. – Vol. IT-22, №. 6. – P. 644–654.

6. Лебедев А. Н. Новая арифметика конечного коммутативного кольца и ее использование в аутентификации / А. Н. Лебедев // Электронные информационные системы. – 2021. – Т. 30, № 3. – С. 49–63.

7. Лебедев А.Н. Обобщение протокола Диффи-Хеллмана с использованием дробно-линейного преобразования / А. Н. Лебедев, А. О. Кокорин // Электронные информационные системы. – 2021. – Т. 30, № 3. – С. 64–71.

8. FIDO Alliance, Fast IDentification Online [Электронный ресурс]. Режим доступа: https://fidoalliance.org. – Дата доступа: 01.10.2021.

УДК 519.7

ЛЕГКОВЕСНЫЙ АЛГОРИТМ ЗАЩИТНОГО КОДИРОВАНИЯ – NASH

Лебедев А.Н., Карондеев А.М., Козлов А.А.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Аннотация. В работе описывается новый легковесный блочный алгоритм защитного кодирования NASH, названный в память выдающегося математика Джона Нэша (John Nash), который кроме работы по экономике, удостоенной нобелевской премии, и работ по чистой математике, удостоенных премии Абеля, занимался также и проблемами защиты информации. Алгоритм NASH при высоком уровне стойкости защитного кодирования показывает также и высокий уровень эффективности при реализации на современных микроконтроллерах.

Ключевые слова. защитное кодирование, блочный алгоритм защитного кодирования, легковесный блочный алгоритм защитного кодирования.

LIGHTWEIGHT SECURE ENCODING ALGORITHM – NASH

Lebedev A., Karondeev A, Kozlov A.

Bauman Moscow State Technical University
Moscow, Russia

Abstract. The paper describes a new lightweight block secure encoding algorithm NASH, which is named in memory of the outstanding mathematician John Nash, who, in addition to his work on economics, awarded the Nobel Prize, and works on pure mathematics, awarded the Abel Prize, was also engaged in the information security. The algorithm NASH having a high security is also a very adaptive to contemporary microcontrollers.

Key words: secure encoding, block secure encoding, lightweight secure encoding, lightweight block secure encoding algorithm.

Адрес для переписки: Лебедев А.Н., 2-я Бауманская ул. 5, стр. 1, г. Москва 105005, Российская Федерация
lebedevan@bmstu.ru

Введение. Термин «кодирование» или «кодирование информации» имеет в современных энциклопедиях, технических словарях и специальных монографиях очень широкую трактовку.

Математическая Энциклопедия, изданная в СССР в 1977–1985 гг. определяет его следующим образом: «Кодирование – процесс представления *информации* в определенной стандартной форме и обратный процесс восстановления информации по ее такому представлению. В математической литературе кодированием называется отображение произвольного множества А в множество конечных последовательностей (слов) в некотором алфавите *B,* а декодированием – обратное отображение» [1].

Из этого общего определения кодирования естественно следует представление, что среди всех возможных кодов (понимаемых как алгорит-

мы кодирования информации) можно выделить отдельные их классы в зависимости от целей использования конкретного процесса кодирования. Так, для передачи информации по теле или радиоканалам применяются коды высокочастотной модуляции, для передачи информации в виде текстов применяется кодирование информации в виде слов как отдельных последовательностей букв алфавита, для передачи информации голосом применяются алгоритмы кодирования с помощью фонем языка, для передачи информации по каналам электросвязи невысокого качества применяются специальные математические коды исправляющие возможные ошибки в канале и т.д.

Среди всех таких классов кодов естественным образом выделяется класс кодов, применяемых именно с целью защиты кодируемой информации от всех, кроме тех, кому она предназначена. Это так называемые защитные коды, среди которых можно выделить более узкий подкласс – шифры. Точные границы класса шифров в классе всех защитных кодов выделить довольно сложно, и мы такой цели в настоящей работе не ставим. Обычно конкретные шифры задаются просто их детальным описанием [2–4].

Структура алгоритма.

Алгоритм защитного кодирования NASH реализует сеть Файстеля [2], в которой последовательно выполняется определенное количество одинаковых по сути преобразований (раундов алгоритма) и на каждом раунде преобразования блока данных изменяется только одна его половина.

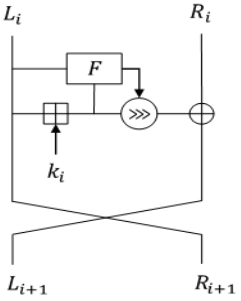

Рисунок 1 – Схема раунда *i* алгоритма NASH

Символами L_i и R_i обозначены левая и правая половинки блока данных, символом k_i обозначен раундовый ключ.

Формулы преобразования блока данных:

$R_{i+1} = L_i$

$L_{i+1} = \left(L_i \boxplus k_i \ggg F(L_i, L_i \boxplus k_i)\right) \oplus R_i$

В последнем раунде половинки выходного блока L_{i+1}, R_{i+1} не меняются местами, то есть:

$L_{i+1} = L_i$

$R_{i+1} = \left(L_i \boxplus k_i \ggg F(L_i, L_i \boxplus k_i)\right) \oplus R_i$

Символом $\boxplus$ обозначается операция сложения двух целых чисел в двоичной записи с забыванием переполнения регистра сумматора, имеющего ту же длину, что и каждый из операндов; символом $\oplus$ обозначается операция XOR; символом REG$\ggg$m обозначается циклический сдвиг регистра REG на m шагов вправо (REG$<<<$ m обозначает циклический сдвиг влево).

Размер блока данных: размер половины блока равен 2^n бит, $n = 4,\ 5$ или 6, т.е. 16, 32 или 64 битам; размер блока – 32, 64 или 128 бит.

Смешивание данных с раундовым ключом. Реализуется операция $\boxplus$ – сложение целых чисел из n бит с приведением результата по модулю 2^n.

Управляемый циклический сдвиг: для блока из 32 бит сдвиг вправо на 5, 8, 6 или 7 бит; для блока из 64 бит сдвиг вправо на 11, 14, 10 или 19 бит; для блока из 128 бит сдвиг вправо на 37, 34, 38 или 29 бит. Значения выбраны на основании проведенного экспериментального анализа.

Функция F управления сдвигами. Интерпретируем содержимое левой половины блока данных L_i как вектор значений булевой функции от n переменных, и *первый выходной бит функции F* получается как значение данной булевой функции на наборе бит двоичного представления числа

$$L_i \boxplus k_i \text{ вида } 2^i - 1, \text{ где } i = 1, \dots, n,$$

то есть как значение

$$L_i\left((L_i \boxplus k_i)[2^1 - 1, \dots, 2^n - 1]\right).$$

Нумерация бит половины блока производится от 0 до $2^n - 1$.

Для размера блока равного 64 битам (половина блока – 32 бита) набор значений величины циклического сдвига следующим образом определяется парами значений булевой функции *F*: 00 – 11; 01 – 14; 10 – 10; 11 – 19.

Число раундов r алгоритма NASH. Число раундов алгоритма защитного кодирования NASH: для блока равного 64 битам $r = 24$; для блока равного 128 битам $r = 28$.

Размер исходного ключа алгоритма. Размер исходного ключа алгоритма NASH: 128, 192 или 256 бит. Исходный ключ может быть получен по любому из алгоритмов работ [3–6]

Проект был реализован в ходе выполнения данным коллективом разработчиков инициативной НИР кафедры ИУ8 (Информационная безопасность) МГТУ им. Н. Э. Баумана (г. Москва) в течение 2016–2020 гг.

Литература

1. Математическая Энциклопедия / И. М. Виноградов (глав редактор) [и др.]. – М. : Советская Энциклопедия, 1979. – Т. 2. – 552 с.

2. Шнайер, Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – Изд. 3-е / Б. Шнайер // М. : Триумф, 2018. – С. 610.

3. Diffie, W. New Directions in Cryptography / W. Diffie, M. E. Hellman // IEEE Trans. Inform. Theory, 1976. – Vol. IT-22, № 6. – P. 644–654.

4. Лебедев, А. Н. Обобщенный протокол Диффи-Хеллмана с аутентификацией сторон / А. Н. Лебедев // Международная алгебраическая конференция, посвященная 110-летию со дня рождения профессора А. Г. Куроша. – М. : МГУ, 2018. – С. 123–127.

5. Лебедев, А.Н. Новая арифметика конечного коммутативного кольца и ее использование в криптографии / А. Н. Лебедев // Электронные информационные системы. – 2021. – Т. 30, № 3. – С. 49–63.

6. Лебедев, А. Н. Обобщение протокола Диффи–Хеллмана с использованием дробно-линей-ного преобразования / А. Н. Лебедев, А. О. Кокорин // Электронные информационные системы, 2021. – № 3 (30).– С. 64–71.

УДК 519.7

НОВЫЙ ПРОТОКОЛ ВЫРАБОТКИ ОБЩЕГО СЕКРЕТА – DHFL

Лебедев А.Н., Кокорин А.О.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Аннотация. Предложены новые однонаправленные функции для обобщения протокола Диффи-Хеллмана. В качестве базового элемента для новых функций использовано дробно-линейное преобразование, для того, чтобы подстановка была определена на всем конечном поле, рассмотрен отдельный случай: ноль в знаменателе. Показано, что протокол на основе введенных однонаправленных функций корректен. Построены обобщения протокола со строгой аутентификацией сторон.

Ключевые слова: новые однонаправленные функции, обобщенный протокол Диффи-Хеллмана, аутентификация, новые арифметические операции, дробно линейные преобразования.

NEW PROTOCOL FOR COMMON SECRET GENERATION - DHFL

Lebedev A., Kokorin A.

Bauman Moscow State Technical University
Moscow, Russia

Abstract. We have proposed some new one way functions for generalization of the Diffie-Hellman protocol. To do this we use any representative of the class of all invertible fractional linear transformations as a basic constructive element for the new functions. In order for the transformation to be defined over the entire finite field, a special case is considered: zero in denominator. We have shown that the protocol based on the constructed one way functions is correct. Generalizations of the protocol with strong authentication of the participants are constructed.

Key words: new one-way functions, generalized Diffie-Hellman protocol, authentication, new arithmetic operations, fractional linear transformations.

Адрес для переписки: Лебедев А.Н., 2-я Бауманская ул. 5, стр. 1, г. Москва 105005, Российская Федерация
lebedevan@bmstu.ru

Введение. Оригинальный протокол Диффи-Хеллмана и его модификации [1, 2], что применяются для формирования общего секрета (ключа взаимной аутентификации) парой пользователей информационной системы (например, сети интернет), использующих для обмена сообщениями общедоступный канал передачи данных, состоят в следующем:

– Пользователи, обозначаемые как *Алиса* и *Боб,* умеют вычислять значения конечных однонаправленных функций $f(x)$, $g(x, y)$;

– функция $f(x)$ определена на некотором конечном множестве X большой мощности и принимает значения из большого конечного множества Y, то есть $f(x)$: $X \to Y$,

– функция $g(x, y)$ определена на декартовом произведении этих множеств $X \times Y$ и принимает значения из третьего большого конечного множества Z, то есть $g(x, y)$: $X \times Y \to Z$,

– стороны независимо выбирают случайные элементы $x1$, $x2$ множества X, вычисляют значения $f(x1)$, $f(x2)$ и обмениваются ими по доступному им каналу связи, например, по сети интернет, то есть передают $f(x1) \leftrightarrow f(x2)$,

– затем они вычисляют общий секрет (ключ, аутентификатор) пары (*Алиса, Боб*) по формулам $K = g(x1, f(x2)) = g(x2, f(x1))$.

– основными, примерами однонаправленных функций $f(x)$ и $g(x, y)$, являются следующие:

– дискретная экспонента по модулю большого простого числа p, то есть при некотором целом числе a, $1 < a < p\text{-}1$, функция $f(x)$ вида

$f: \mathbb{Z}_{p-1} \to \mathbb{Z}_p;$ $\quad f(x) = a^x \pmod p$,

и функция $g(x, y)$

$g(x, y)$: $\mathbb{Z}_{p-1} \times \mathbb{Z}_p \to \mathbb{Z}_p$; $g(x, y) = y^x \pmod p$.

В этом случае общий секрет данной пары пользователей (ключ, аутентификатор) вычисляется по формуле $K = g(x1, f(x2)) = f(x2)^{x1} \pmod p = g(x2, f(x1)) = f(x1)^{x2} \pmod p$;

$K = a^{x1x2\ (mod\ p-1)} \pmod p = a^{x2x1\ (\mathrm{mod}\ p-1)} \pmod p$,

и представляется элементом мультипликативной группы $\mathbb{Z}_p^*$ большого простого поля $\mathbb{Z}_p$. Такой протокол обычно обозначается как DH [1].