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].

– Во-вторых, это вычисление кратной точки некоторой эллиптической кривой над большим конечным полем $\mathbb{F}$

$E_{a,b}(p) = \{(x, y)|\ x, y \in \mathbb{F}, y^2 = x^3 + ax + b\ (\mathbb{F})\}$.

Пусть $P = (x, y) \in E_{a,b}(\mathbb{F})$ – точка большого порядка кривой $E_{a,b}(\mathbb{F})$, тогда функции $f(n)$ и $g(n, Q)$ определяются как $f(n)$: $\mathbb{Z}_q \to E_{a,b}(\mathbb{F})$, где $q = |<P>|$ – порядок циклической подгруппы, порожденной точкой P в группе $E_{a,b}(\mathbb{F})$, функция $g(n, Q)$: $\mathbb{Z}_q \times E_{a,b}(\mathbb{F}) \to E_{a,b}(\mathbb{F})$, такова, что значениями обеих функций $f(x)$ и $g(x, y)$ будут точки кривой $E_{a,b}(\mathbb{F})$ $f(n) = nP = P+P+...+P$; $g(n, f(m)) = n(mP) = mP+mP+...+mP = (mn)P$,и общий секрет пары также будет точкой $E_{a,b}(\mathbb{F})$ и вычисляется по формуле $K = g(n, f(m)) = n(mP) = g(m, f(n)) = m(nP) = (mn)P$.

Этот общий секрет представляется элементом циклической подгруппы $<P>$ группы точек кривой $E_{a,b}(\mathbb{F})$ над полем $\mathbb{F}$, порожденной точкой P, выбираемой так, что порядок группы $|<P>| = q$ – также большое простое число. Такой протокол обозначается как ECDH [4, 5]. Главный недостаток оригинального протокола Диффи-Хеллмана (DH) и его модификации ECDH, – отсутствие аутентификации сторон [3–5]. Поэтому за 45 лет предложено несколько вариантов усложнения этого протокола для получения протокола выработки общего секрета (ключа, аутентификатора) с взаимной аутентификацией сторон [4, 6–10].

В работах [1, 2] предложен новый общий метод формирования общего секрета (ключа, кода, аутентификатора) парой пользователей информационной системы (в частности, сети интернет), радикально расширяющий известные варианты протокола Диффи-Хеллмана и его обобщений, как его оригинального варианта, так и его модификаций с взаимной аутентификацией сторон или с аутентификацией только одной из них.

В данной работе мы реализуем один из вариантов этого метода, основанный на использовании новых арифметических операций в кольце показателей дискретной экспоненты или кольце кратностей выделенной точки эллиптической кривой над большим конечным полем, базирующихся на использовании одного конкретного класса легко реализуемых подстановок – класса взаимно однозначных дробно-линейных преобразований.

Предлагаются функции $f(x)$, $g(x, y)$ построенные на взаимно однозначном дробно-линейном преобразовании в показателях дискретной экспоненты над большим простым полем $\mathbb{Z}_p$, или взаимно однозначном дробно-линейном преобразовании в показателе кратности некоторой заданной заранее точки $P \in E_{a,b}(\mathbb{F})$ в группе точек эллиптической кривой над большим конечным полем $\mathbb{F}$, $E_{a,b}(p) = \{(x, y)|\ x, y \in \mathbb{F}, y^2 = x^3 + ax + b\ (\mathbb{F})\}$.

Идея использования дробно-линейного взаимно однозначного преобразования именно для этой цели была впервые высказана в работах первого из авторов настоящей статьи [1, 2].

Протокол DHFL.

Поскольку новая операция умножения $\otimes$ ассоциативна, то возможна перестановка скобок, а перестановкой скобок доказывается равенство:

$$K = K1 = Q2 \otimes Q2 \otimes \ \otimes Q2 = K2 = Q1 \otimes Q1 \otimes \ \otimes Q1$$

Таким образом, получившийся алгоритм корректен.

Таблица 1.

Шаг	Информация *Алисы*	Информация *Боба*
1	Случайно выбирает $x1$ $x1 \in X$	Случайно выбирает $x2$ $x2 \in X$
2	Вычисляет элемент $Q1 = g \otimes g \otimes \ \otimes g$ *«умножая его»* $x1$ раз	Вычисляет элемент $Q2 = g \otimes g \otimes \ \otimes g$ *«умножая его»* $x2$ раз
3	Получает от партнера $Q2 = g \otimes g \otimes \ \otimes g$ *«умноженный»* $x2$ раз	Получает от партнера $Q1 = g \otimes g \otimes \ \otimes g$ *«умноженный»* $x1$ раз
4	Вычисляет элемент $K1 = Q2 \otimes Q2 \otimes \ \otimes Q2$ *«умножая его»* $x1$ раз	Вычисляет элемент $K2 = Q1 \otimes Q1 \otimes \ \otimes Q1$ *«умножая его»* $x2$ раз

Литература

1. 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.

2. 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.

УДК 621.317.7

НЕКОТОРЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ ПАССИВНЫХ ФИЛЬТРОВ ДЛЯ ФОРМИРОВАНИЯ ОПОРНЫХ СИГНАЛОВ

Левко И.А.

Белорусский государственный университет
Минск, Республика Беларусь

Аннотация. Рассмотрен один из подходов к формированию опорных сигналов синусоидальной формы с использованием импульсных сигналов и пассивных ФНЧ. Показано, что реализация ФНЧ на практике требует не только проведения расчета с использованием специальных таблиц, но и применения программ моделирования электронных схем.

Ключевые слова: опорный синусоидальный сигнал, ФНЧ, нормированный фильтр, программа моделирования электронных схем.