DOI 10.37882/2223–2966.2022.11.19

ЗАЩИТА ПЕРЕДАЧИ ПРОСТРАНСТВЕННО-ВРЕМЕННЫХ ДАННЫХ С ПРИМЕНЕНИЕМ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ НА ГРУППАХ ПРИ МОДЕЛИРОВАНИИ РАСПРОСТРАНЕНИЯ ВОЛН С ИСПОЛЬЗОВАНИЕМ СПЛЕТЕНИЙ ГРУПП

PROTECTION OF THE TRANSMISSION OF SPATIO-TIME DATA WITH THE USE OF CRYPTOGRAPHIC PROTOCOLS ON GROUPS IN MODELING WAVE PROPAGATION USING REGULAR WREATH PRODUCT OF GROUPS.

K. Lossov

Summary. The article proposes a new approach to protecting the transmission of spatio-temporal data during wave propagation. This approach is based on the modeling of wave phenomena, using the theoretical — group construction of the regular wreath product of groups. This makes it possible to encrypt the information transmitted by the wave using the methods of algebraic cryptography.

Keywords: spatiotemporal data, encryption, wave propagation, group, conjugate element, Cartesian product of groups, direct product of groups, regular wreath product of groups, digital signal, analog signal.

Лоссов Константин Иванович
Московский государственный университет геодезии и картографии
konsiv@gmail.com

Аннотация. В статье предложен новый подход к защите передачи пространственно –временных данных при распространении волн. В основе этого подхода лежит моделирование волновых явлений, использующее теоретико — групповую конструкцию сплетения групп. Это позволяет для шифрования информации, передаваемой волной, использовать методы алгебраической криптографии.

Ключевые слова: пространственно–временные данные, шифрование, распространение волн, группа, сопряженный элемент, декартово произведение групп, прямое произведение групп, декартово сплетение групп, прямое сплетение групп, цифровой сигнал, аналоговый сигнал.

«Необходимость защиты информации, передаваемой по современным сетям, а также огромные возможности ее взлома и искажения, обусловленные развитием компьютерной техники, требуют совершенно нового подхода к защите информации, новых методов шифрования. Замечательно, что при этом используется современная математика» [1].

Оказывается, что для описания волновых явлений можно использовать аппарат теории групп, а именно, конструкцию сплетения, введенную В.А. Калужниным [2], после чего для шифрования информации передаваемой волной, можно, в частности, использовать некоторые криптографические протоколы на группах, основы которых изложены в монографии [3].

Пусть X и Y — некоторые множества, тогда их прямым произведением называется множество X × Y элементами которого являются упорядоченные пары (x, y) для всевозможных $x \in X$ и $y \in Y$, т.е.

$$X \times Y = \{(x, y) | x \in X, y \in Y\}.$$

Бинарной операцией на множестве X называют отображение

$$P: X \times X \to X.$$

Множество G называется группой, если выполнены следующие аксиомы

1. на множестве определена бинарная операция: $(x, y) \mapsto xy$;
2. операция ассоциативна: $(xy)z = x(yz)$ для всех $x, y, z \in G$;
3. G обладает единичным элементом e: $xe = ex = x$ *для всех* $x \in G$;
4. для каждого элемента $x \in G$ существует обратный x^{-1}:

$$x x^{-1} = x^{-1} x = e.$$

Пусть $\{G_i, i \in I\}$ — некоторое бесконечное семейство групп, тогда их декартовым произведением $\overline{\Pi}_{i \in I} G_i$ называется группа, состоящая из всевозможных функций:

$f: I \to \bigcup_{i \in I} G_i$, где $f(i) \in G_i$;

с операцией умножения $(f_1 * f_2) * (i) = f_1(i) * f_2(i)$, где $f_1(i), f_2(i)$ — элементы группы G_i, $f_1: I \to \bigcup_{i \in I} G_i$, $f_2: I \to \bigcup_{i \in I} G_i$

Единицей группы $\overline{\prod}_{i \in I} G_i$ будет функция $f_e: I \to \bigcup_{i \in I} G_i$ такая, что $f(i) = e_i$, где e_i — единица группы G_i, $i \in I$.

Носителем функции f называется множество $supp(f)$ тех индексов i, для которых $f(i) \neq e_i$:

$$supp(f) = \{i \in I | f(i) \neq e_i\}$$

Подгруппа $\prod_{i \in I} G_i$ группы $\overline{\prod}_{i \in I} G_i$, состоящая из всех элементов $f \in \overline{\prod}_{i \in I} G_i$ с конечным носителем, называется прямым произведением групп G_i, $i \in I$.

Дадим теперь определение теоретико-групповой конструкции сплетения в редакции, изложенной в [4].

Пусть существуют A и B группы. Обозначим $Fun(B, A)$, $fun(B, A)$, декартово произведение и прямое произведение изоморфных копий группы A из определений данных выше, где $I = B$.

Таким образом, $Fun(B, A)$, $fun(B, A)$ — декартово произведение и прямое произведение изоморфных копий группы A, индексированных элементами группы B. Символически это можно изобразить следующим образом:

A, ... * A * ... — произведение изоморфных копий группы A,

b_1, ... b_i ... — индексы.

$f \in Fun(B, A)$ выглядит как

a_1, ... a_i ... — значения функции,

b_1, ... b_i ... — значения аргумента.

Для функции $f \in fun(B, A)$ лишь конечное число a_i отлично от e_A (единицы группы A).

Декартовым сплетением AWrB группы A и B называется множество $B * Fun(B, A)$ с умножением

$$bf * b'f' = bb' * f^{b'}f', \text{ где } f^b(x) = f(bx). \quad (1)$$

Нетрудно проверить, что AWrB с введенной в (1) операций умножения является группой с единицей $e_B e_F$, где e_B — единица группы B, а $e_F: B \to \bigcup_{b \in B} A_b$, $e_F(b) = e_A, \forall b \in B$.

Прямым сплетением AwrB группы A и B называется подгруппа $B * fun(B, A)$ группы AWrB.

Элементы a и b группы G называются сопряженными в этой группе, если существует хотя бы один элемент $h \in G$, что

$$b = h^{-1}ah.$$

Утверждение. Пусть e_F — единица группы $Fun(B, A)$, e_B — единица группы B, тогда

$$b^{-1}e_F * e_B f * be_F = e_B * f^b(x) \quad (2)$$

Если be_F отождествлять с b, а $e_B f$ с f, то (2) можно переписать в виде

$$b^{-1}fb = f^b, \text{ где } f^b(x) = f(bx). \quad (3)$$

Таким образом, f и f^b сопряжены при помощи элемента b.

Если C и D — два подмножества группы G, то C^D обозначает множество элементов $d^{-1}c\,d$, где $c \in C, d \in D$:

$$C^D = \{d^{-1}c\,d | c \in C, d \in D\} \quad (4)$$

Будем говорить, что группа G циклическая, если существует такой элемент a в G, что всякий элемент x из G может быть представлен в виде a^n, где $n \in \mathbb{Z}$.

Пусть G и G' — группы. Гомоморфизм групп G в G' — это отображение $f: G \to G'$, удовлетворяющее условию $f(xy) = f(x)f(y)$ для всех $x, y \in G$ и единицу группы G в единицу группы G'. Если f при этом является взаимно однозначным отображением (биекцией), то f называют изоморфизмом.

Если $G = G'$, то мы говорим, что изоморфизм есть автоморфизм.

Гомоморфизм $f: G \to G'$, устанавливающий изоморфизм между группой G и ее образом в G', мы будем называть вложением.

Вообще говоря, не существует общего определения волн. Д. Уизем в [5] предлагает руководствоваться следующим «интуитивным представлением о волне как о любом различимом сигнале, передающимся от одной части среды к другой с некоторой определенной скоростью. Такой сигнал может быть возмущением любого вида, например максимумом какой — либо величины или резким ее изменением при условии, что в любой заданный момент времени можно определить его местонахождение. Этот сигнал может искажаться, изменять свою величину и скорость, но при этом должен оставаться различимым».

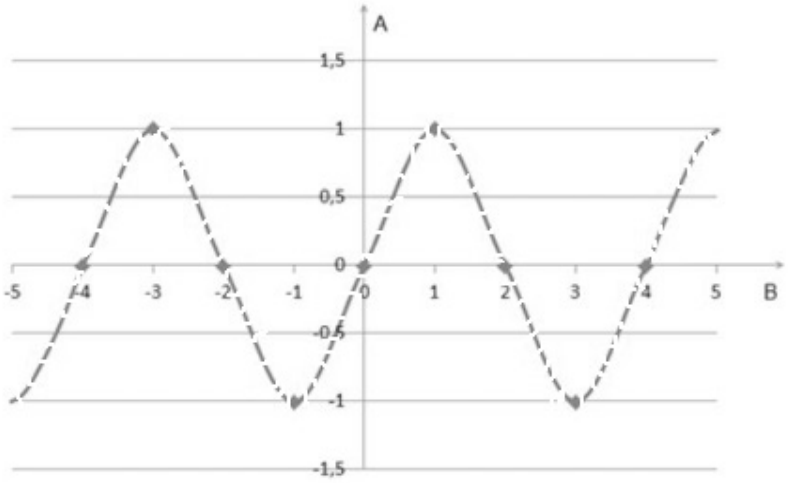

Рис. 1. Профиль волны в начальный момент времени

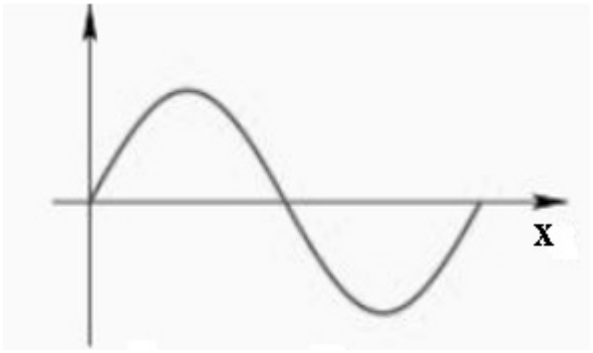

Рис. 2. Непрерывный сигнал

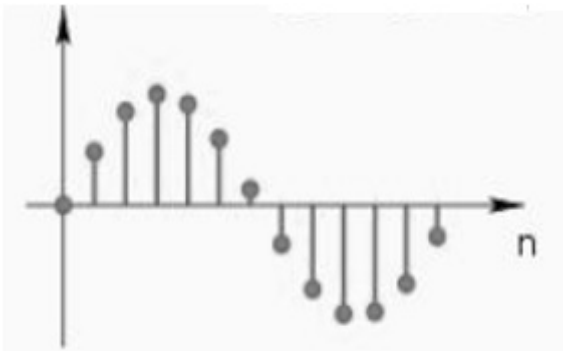

Рис. 3. Сигнал после дискретизации

Пусть A и B группы и AWrB их декартово сплетение, b — некоторый элемент группы B, а f произвольный элемент $Fun(B,A)$.

Множество $\{f\}^{(b)}$ в смысле определения (4), где (b) — циклическая группа, порожденная элементом b, принадлежащее AWrB, можно рассматривать как волну с формой, описываемой функцией f, движущуюся со скоростью b. Действительно, если в качестве оси OX взять группу B, а группу A рассматривать как ось OY, при этом вместо шкалы времени использовать $\mathbb{N} \cup \{0\}$ (discrete time). Тогда, считая что в начальный

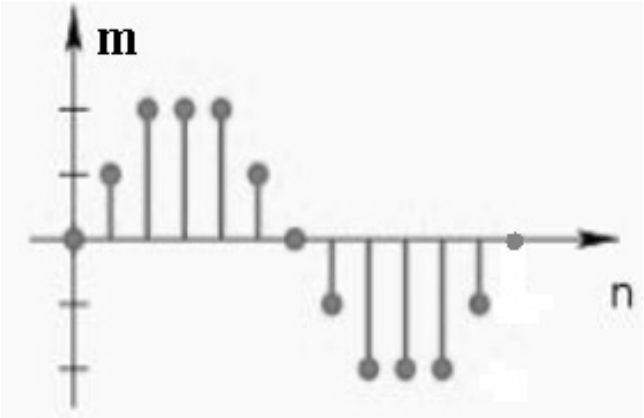

Рис. 4. Сигнал после дискретизации и квантования

момент времени (t=0) профиль волны задан элементом $f \in Fun(B,A)$, полагаем что через к единиц времени профиль описывается элементом $b^{-k}fb^{k} \in \{f\}^{(b)}$, сопряженным f при помощи элемента b^k, который согласно (3) равен f^{b^k}, где $f^{b^k}(x) = f(b^k x)$.

Пример. Пусть $A = B = (\mathbb{Z}, +, 0)$, где $(\mathbb{Z}, +, 0)$ — группа целых чисел по сложению, таким образом, $AWrB = \mathbb{Z}Wr\mathbb{Z}$, и пусть $f \in Fun(B,A)$:

$$f(n) = \sin\frac{n\pi}{2}, n \in \mathbb{Z}$$

задает профиль волны в начальный момент времени (t=0), который символически можно изобразить следующим рисунком.

При $b = m \in \mathbb{Z}$, $m > 0$ $(m < 0)$ через k единиц времени график функции изображенный на рисунке 1 сдвинется на km единиц влево (вправо), поскольку

$$f^{kb}(n) = \sin\frac{(n+km)n}{2}.$$

Более общо, группа $\mathbb{Z}Wr\mathbb{Z}$, в рамках вышеизложенной модели, может использоваться для описания цифрового сигнала произвольного профиля, движущегося с постоянной скоростью, получающегося из непрерывного после дискретизации и квантования.

Кроме того, известно [4], что сплетение $\mathbb{Z}wr\mathbb{Z}$ изоморфно подгруппе, порожденной в $GL_2(R)$ матрицами

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix},$$

где ζ — трансцендентное действительное число. Таким образом, в этом случае можно использовать, например, протокол разделения ключа Романчука-Устименко [6].

В общем случае для шифрования волны $\{f\}^{(b)}$ удобно использовать криптографический протокол Habeeb — Kahrobaei — Koupparis — Shpilrain [6], который использует понятие голоморфа группы.

Пусть G — группа, а Aut (G) — группа ее автоморфизмов. Тогда голоморфом Hol(G) называется множество Aut (G) G на котором операция умножения задается следующим равенством:

$$\varphi g * \varphi' g' = \varphi\varphi' * \varphi'(g)g' \quad (5)$$

Так как имеется естественное вложение $B \to Aut(Fun(B,A))$ (Bээ$b \longrightarrow \hat{b}$, где $\hat{b} \in Aut(Fun(B,A))$ действует по правилу: $f \longrightarrow f^{b}, f \in Fun(B, A)$, см. (3)), то сравнивая (1) и (5), легко заметить, что AWrB является подгруппой $Hol(Fun(B,A))$.

Корреспонденты X и Y выбирают открыто группу G — платформу протокола, автоморфизм φ ∈ Aut (G) и элемент $f \in G$. Группа G, автоморфизм φ и элемент g — открытый ключ.

X "случайным образом" выбирает секретное (private) натуральное число m ∈ N, вычисляет элемент голоморфа Hol(G)

$$(\varphi, g)^m = (\varphi^m, \varphi^{m-1}(g) \cdot \varphi^{m-2}(g) \cdot \ldots \cdot \varphi^2(g) \cdot \varphi(g) \cdot g)$$

и пересылает Y только вторую компоненту

$$a_m = \varphi^{m-1}(g) \cdot \varphi^{m-2}(g) \cdot \ldots \cdot \varphi^2(g) \cdot \varphi(g) \cdot g.$$

Y "случайным образом" выбирает секретное (private) натуральное число n ∈ N, вычисляет элемент голоморфа Hol(G)

$(\varphi, g)^n = (\varphi^n, \varphi^{n-1}(g) \cdot \varphi^{n-2}(g) \cdot \ldots \cdot \varphi^2(g) \cdot \varphi(g) \cdot g)$ и пересылает X только вторую компоненту $a_n = \varphi^{n-1}(g) \cdot \varphi^{n-2}(g) \cdot \ldots \cdot \varphi^2(g) \cdot \varphi(g) \cdot g$.

Выработка общего секретного ключа X вычисляет элемент

$(*, a_n) \cdot (\varphi^m, a_m) = (* \cdot \varphi^m, \varphi^m(a_n) \cdot a_m) = (* \cdot \varphi^m, a_{n+m})$.
$KX = a_{n+m}$.

Y вычисляет элемент

$(**, a_m) \cdot (\varphi^n, a_n) = (* * \cdot \varphi^n, \varphi^n(a_m) \cdot a_n) = (* * \cdot \varphi^n, a_{m+n})$.
$KY = a_{m+n}$.

Общий секретный ключ $K = KX = a_{n+m} = a_{m+n} = KY$.

Для шифрования волны в качестве группы G следует выбрать $Hol(Fun(B,A))$.

Криптостойкость системы основана на трудноразрешимой задаче нахождения по элементу $h^{-1}ah$ и элементу a сопрягающего элемента h. Поскольку волна задается подмножеством AWrB, а ключ шифрования является элементом $Hol(Fun(B,A))$, то шифрование применяется непосредственно к волне. Таким образом, например, если в качестве групп A и B взять R, то можно при помощи криптографических протоколов основанных на группах шифровать аналоговые сигналы.

ЛИТЕРАТУРА

1. В.А. Романьков. Введение в криптографию. М.: ФОРУМ, 2012.
2. Л.А. Калужнин Sur les p-groupes de Sylow du groupe symetrique du degre p^m, C.R. Paris 221 (1945), 222–224.
3. Myasnikov A., Shpilrain V., Ushakov A. Group-based cryptography. Advanced courses in mathematics CRM Barselona.— Basel-Boston-Berlin: Birkhauser, 2008.
4. М.И. Каргаполов, Ю.И. Мерзляков. Основы теории групп. Москва «Наука», 1982
5. Дж. Уизем. Линейные и нелинейные волны. Москва. Мир, 1977.
6. В.А. Романьков. Алгебраическая криптография: монография. Омск. Изд-во Омского. гос. университета, 2013.
7. С. Ленг. Алгебра. М.: «Наука», 1965.

Журнал «Современная наука: актуальные проблемы теории и практики»