О Б О З Р Е Н И Е
П Р И К Л А Д Н О Й И П Р О М Ы Ш Л Е Н Н О Й
Том 30 М А Т Е М А Т И К И Выпуск 1
2023

С. Ю. К а т ы ш е в, **А. И. З о б о в**, **Н. А. К а р ю к** (Москва, МИРЭА). **Исследование принципов применения неассоциативных алгебраических структур при синтезе асимметричных криптографических механизмов.**

УДК 512.548.2 DOI https://doi.org/10.52513/08698325_2023_30_1_1

Резюме: В данной работе представлен алгоритм открытого распределения ключей основанный на парамедиальных квазигруппах, который потенциально является более стойким, нежели алгоритм распределения ключей над ассоциативными структурами.

Ключевые слова: Парамедиальные квазигруппы, криптография с открытым ключом, алгоритм Диффи-Хеллмана, открытое распределение ключей.

В данной работе предлагается алгоритм открытого распределения ключей основанный на парамедиальных квазигруппах. Впервые алгоритм открытого распределения ключей был представлен в работе Диффи-Хеллмана [1] в 1976 году.

В общем виде его можно представить следующим образом.

Алгоритм. Пусть $(G,*)$ — произвольный конечный группоид, $\mathfrak{L}_A, \mathfrak{L}_B$ — некоторые поэлементно перестановочные подмножества его преобразований (чаще эндоморфизмов), g элемент группоида $(G,*)$. Абоненты A и B независимо друг от друга выбирают произвольные эндоморфизмы $\rho_A \in \mathfrak{L}_A$, $\rho_B \in \mathfrak{L}_B$, соответственно, и обмениваются элементами g^{ρ_A} и g^{ρ_B}. Затем формируют общий секретный ключ

$$g^{\rho_A\rho_B} = g^{\rho_B\rho_A}.$$

Такого рода алгоритмы рассматривались в работах С. Ю. Катышева, В. Т. Маркова, А. А. Нечаева [2], В. Т. Маркова [3] и других. В частности, в качестве G использовали:

— лупы Муфанга,

— медиальные квазигруппы,

— конечномерные алгебры над полем.

О п р е д е л е н и е 1. Квазигруппа $(G,*)$ называется парамедиальной, если для любых $x,y,u,v \in G$

$$(x*y)*(u*v) = (v*y)*(u*x).$$

О п р е д е л е н и е 2. Зафиксируем элемент g квазигруппы $(G,*)$, тогда правая степень определяется следующим образом: $g^1 = g$, $g^n = \underbrace{((...(g*g)*...)*g)}_{n \text{ - сомножителей}}$,

$g^{P+Q} = g^P * g^Q$,
$g^{P*n} = \underbrace{((...(g^P * g^P) * ...) * g^P)}_{n \text{ - сомножителей}}$.

Индуктивно определим симметричную степень:

$$g^{\overline{1}} = g = g^1, \quad g^{\overline{n}} = \underbrace{(g*(...*(g*g)...))}_{n \text{ - сомножителей}}, \quad g^{\overline{P+Q}} = g^{\overline{Q}} * g^{\overline{P}},$$

$$g^{\overline{P*n}} = \underbrace{(g^{\overline{P}}*(...*(g^{\overline{P}}*g^{\overline{P}})...))}_{n \text{ - сомножителей}}.$$

Обозначим n-ю степень элемента $g \in G$ с расстановкой скобок a_n и высотой дерева k, как $g^{(n,a_n^k)}$, а симметричную ей степень обозначать, как $g^{(n,\bar{a}_n^k)}$.

Высота листа — расстояние до корня.

Высота дерева — максимальная высота листа.

Теорема 1. *Для любых $g,h \in G$, где $(G,*)$ — парамедиальная квазигруппа, и для любой степени (n,a_n^k), такой что все листы имеют четную высоту, $n,k \in \mathbb{N}$ получим*:

1) $(g*h)^{(n,a_n^{2k+1})} = h^{(n,\bar{a}_n^{2k+1})} * g^{(n,\bar{a}_n^{2k+1})}$
2) $(g*h)^{(n,a_n^{2k})} = g^{(n,\bar{a}_n^{2k})} * h^{(n,\bar{a}_n^{2k})}$

Теорема 2. *Для любого $g \in G$, где $(G,*)$ — парамедиальная квазигруппа, и любой степени (n,a_n^k), (m,a_m^t), таких что все все листы имеют четную высоту, $n,m,k,t \in \mathbb{N}$ получим*:

1) $(g^{(m,a_m^{2t})})^{(n,a_n^{2k})} = (g^{(n,a_n^{2k})})^{(m,a_m^{2t})}$
2) $(g^{(m,a_m^{2t+1})})^{(n,a_n^{2k})} = (g^{(n,\bar{a}_n^{2k})})^{(m,a_m^{2t+1})}$
3) $(g^{(m,a_m^{2t})})^{(n,a_n^{2k+1})} = (g^{(n,a_n^{2k+1})})^{(m,\bar{a}_m^{2t})}$
4) $(g^{(m,a_m^{2t+1})})^{(n,a_n^{2k+1})} = (g^{(n,\bar{a}_n^{2k+1})})^{(m,\bar{a}_m^{2t+1})}$

С учетом теоремы 2 алгоритм открытого распределения ключей может быть сформулирован следующим образом:

Алгоритм. Выбирается (несекретный) элемент g парамедиальной квазигруппы $(G,*)$.

Абонент А выбирает произвольную степень (n,a_n^{2k}) и отправляет абоненту В:

$$g^{(n,a_n^{2k})}.$$

Абонент В выбирает произвольную степень (m,a_m^{2t+1}) и отправляет абоненту А:

$$g^{(m,a_m^{2t+1})}.$$

Затем А и В формирует общий ключ К:

$$K_A = (g^{(m,a_m^{2t+1})})^{(n,\bar{a}_n^{2k})} = (g^{(n,a_n^{2k})})^{(m,a_m^{2t+1})} = K_B.$$

По теореме 2 могут быть составлены еще 3 варианта алгоритма открытого распределения ключей.

СПИСОК ЛИТЕРАТУРЫ

1. *Diffie W., Hellman M. E.* New directions in cryptography. — IEEE Trans. Inform. Theory, 1976, v. 22, p. 644–654.
2. *Катышев С. Ю., Марков А. А., Нечаев А. А.* Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей. — Дискретн. матем., 2014, т. 26, в. 3, с. 45-64.// *Katyshev S. Yu., Markov V. T., Nechaev A. A.*, Application of non-associative groupoids to the realization of an open key distribution procedure. — Discrete Math. Appl., 2015, v. 25, 1, p. 9–24.
3. *Марков В. Т., Михалев А. В., Грибов А. В. и др.* Квазигруппы и кольца в кодировании и построении криптосхем. — Прикладная дискретная математика, 2012, т. 18, № 4, с. 32–52.// *Markov V. T., Mihalev A. V., Gribov A. V. and other.* Quasigroups and rings in coding and crypto schemes construction. — Discrete Math., 2012, v. 18, № 4, p. 32–52.

Поступила в редакцию
3.X.2023

UDC 512.548.2 DOI https://doi.org/10.52513/08698325_2023_30_1_1

Katyshev S. Yu., ***Zobov A. I.*** , ***Karyuk N. A.*** (Moscow, MIREA)**. Exploring the Principles of Non-Associative Algebraic Structures in the Synthesis of Asymmetric Cryptographic Mechanisms.**

Abstract: In this paper the algorithm for public key exchange based on paramedial quasigroups is presented, which potentially offers increased resilience compared to key distribution algorithms over associative structures.

Keywords: Paramedial quasi - groups, public key cryptography, Diffie-Hellman key exchange.