2. Kohlhase M. *OMDoc: An Open Markup Format for Mathematical Documents [version 1.2]* // Lecture Notes in Artificial Intelligence. – 2006. – V. 4180. – 428 p.

3. Kohlhase M. *Using LaTeX as a Semantic Markup Format*. URL: https://kwarc.info/kohlhase/papers/mcs08-stex.pdf.

4. *KWARC: Knowledge Adaptation and Reasoning for Content*. URL: https://kwarc.info/

5. Kohlhase M., David C., Ginev D., Cornely J. *eMath 3.0: Building Blocks for a Social and Semantic Web for Online Mathematics & eLearning* // Computer Science, Jacobs University Bremen, Germany. – October 27, 2010. – 14 p.

6. Kohlhase M., Iancu M. *Co-Representing Structure and Meaning of Mathematical Documents* // Computer Science, Jacobs University Bremen, Germany. – October 26, 2015. – 24 p.

7. Kohlhase M. *OMDoc: An Open Markup Format for Mathematical Documents* // FB Informatik, Universitat des Saarlandes D-66041 Saarbrucken, Germany. – 2000. – 64 p.

8. Елизаров А.М., Липачев Е.К., Малахальцев М.А. *Веб-технологии для математика: основы MathML. Практическое руководство* // М.: ФИЗМАТЛИТ, 2010. – 192 с.

9. Елизаров А.М., Липачев Е.К., Малахальцев М.А. *Языки разметки семантического веба. Практические аспекты*. – Казань, 2008.

10. Елизаров А. М., Липачев Е. К., Малахальцев М.А. *Основы MATHML. Представление математических текстов в Internet*. – Казань, 2008.

METHOD OF SEMANTIC REPRESENTATION DIGITAL MATHEMATIC DOCUMENTS

P.O. Gafurova

Several works of semantic representation of mathematical documents was reviewed. We also designed the language of semantic representation of mathematical documents, serviced the processing of this language and possibilites for its semantic search and representation of the given language.

Keywords: semantic Web, semantic, OMDoc, semantic representation of mathematics documents.

УДК 519.7; 512.581

О МАСКИРОВКЕ АЛГЕБРАИЧЕСКИХ ПЛАТФОРМ В КРИПТОГРАФИИ С ОТКРЫТЫМ КЛЮЧОМ

К.И. Емельянов[1]

1 *kirillemelyanov11041995@gmail.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

В статье обсуждается маскировка алгебраических платформ, таких как группы и группоиды. Идея подобной маскировка переносится на более сложную платформу – 2-категорию.

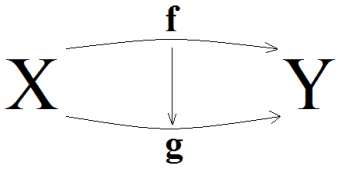
Ключевые слова: криптография, маскировка алгебраических платформ, 2-категория.

В работе [1] был предложен метод маскировки алгебраических платформ, позволяющий при некоторых предположениях гарантировать невзламываемость криптографических протоколов в течение любого наперед заданного времени. В работе [2] были описаны некоторые приложения этого метода.

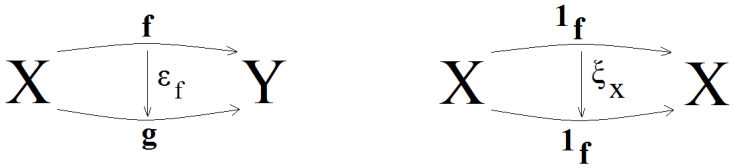
Смысл маскировки в том, что прежде чем противник сможет атаковать криптографический протокол, он должен будет найти некий маскирующий элемент c. Но для этого ему понадобится время, которое можно сделать любым наперед заданным. В группе G можно ввести маскирующий элемент $c \in G$, который будет заменять определённую в группе операцию умножения. Например, это можно сделать таким образом: $a * b = acb$. В результате получается группа $G(c)$ с новой единицей c^{-1}: $a^{-1} = c^{-1}a^{-1}c^{-1}$. Очевидно, эту группу также можно маскировать. Отметим, что $G \cong G(c)$.

В [1] показано, как аналогичным способом можно маскировать группоиды, то есть категории, в которых каждый морфизм обратим. Оказалось также, что похожая конструкция позволяет указать общий способ построения произвольных группоидов. Наша цель в данной работе — описать метод маскировки для принципиально новой для криптографии алгебраической платформы — 2-категорий.

Напомним, что такое 2-категория (см. [3], [4]). Пусть K — категория с объектами X, Y, Z, ... и морфизмами f, g, h, ... (1-морфизмы). Пусть для каждой пары X, Y множество морфизмов $K(X, Y)$ само является категорией, объекты которой — 1-морфизмы. Морфизмы этой категории (морфизмы между 1-морфизмами) будут называться 2-морфизмами и обозначаться так:



Для 2-морфизмов определены два вида суперпозиций, вертикальные и горизонтальные. Горизонтальные суперпозиции будем обозначать так: $\alpha_2 \circ \alpha_1$. Относительно каждой суперпозиции существуют единицы. Обозначим вертикальную единицу через ε_f, а горизонтальную — через ξ_x. Графически их можно изобразить так:

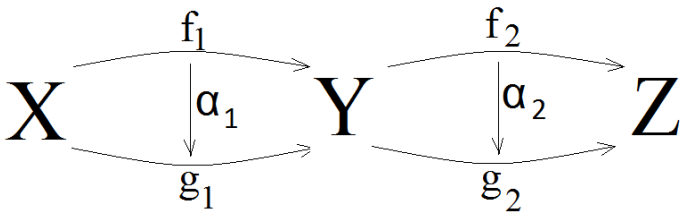


Можно замаскировать вертикальную, горизонтальную или обе композиции одновременно. Замаскируем, например, горизонтальную композицию.

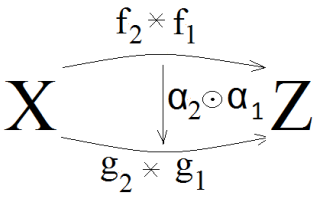
Для каждого объекта Y (1-категории) выбирается маскирующий *обратимый* 1-морфизм $c_Y : Y \to Y$. Это даст маскировку в 1-категории K: вместо суперпозиции gf появляется $g * f = gc_Y f$. Графически:

$$X \xrightarrow{f} Y \xrightarrow{c_Y} Y \xrightarrow{g} Z$$

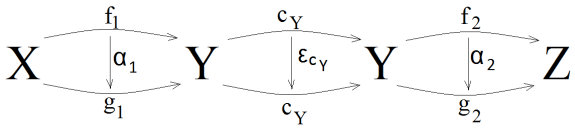
Определим новую горизонтальную суперпозицию 2-морфизмов α_1 и α_2:



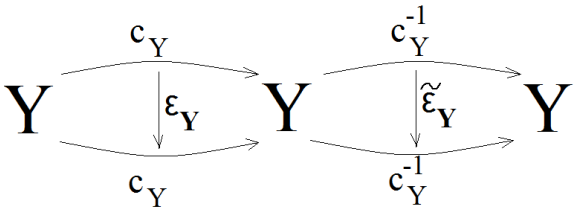
Результат должен иметь вид:



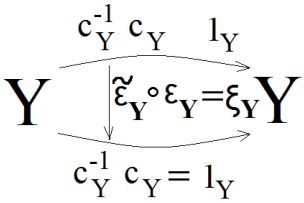
Точное определение: $\alpha_2 \odot \alpha_1 = \alpha_2 \circ \varepsilon_Y \circ \alpha_1$.



Через ε_Y здесь обозначена вертикальная единица ε_{c_Y} Необходимо потребовать обратимость каждого ϵ_Y относительно горизонтальной композиции. То есть должны существовать 2-морфизмы $\tilde{\varepsilon}_Y$



такие, что $\tilde{\varepsilon}_Y \circ \varepsilon_Y = \xi_Y$, $\varepsilon_Y \circ \tilde{\varepsilon}_Y = \xi_Y$:



Так как в $K_{(c)}$ как 1-категории единичные 1-морфизмы – это c_Y^{-1}, то в замаскированной 2-категории горизонтальные единицы – это $\tilde{\varepsilon}_Y$.

Вертикальная суперпозиция останется той же самой. В результате получаем новую (замаскированную) 2-категорию $K_{(c)}$, эквивалентную исходной. Но без знания маскирующих морфизмов вычисления в ней оказываются невозможными. В

дальнейшем эта конструкция будет, как и в [1], [2], использована для обеспечения криптостойкости криптографических протоколов.

Литература

1. Gaynullina, A. R., Tronin S. N. *Some New Platforms for Algebraic Cryptography and One Method of Increasing the Security* // Lobachevskii Journal of Mathematics. – 2016. – V. 37. – No. 6. – P. 768–776.

2. Емельянов К. И. *Использование групп матриц и соответствующих им категорных группоидов для конструирования криптографических протоколов* – Бакалаврская выпускная работа. – Казань, 2016.

3. Маклейн С. *Категории для работающего математика.* – М.: ФИЗМАТЛИТ, 2004. – 352 с.

4. Кондратьев Г. В. *Категории и некоторые их приложения.* – М.: ИНФРА-М, 2017. – 174 с.

ON THE MASKING OF ALGEBRAIC PLATFORMS IN PUBLIC KEY CRYPTOGRAPHY

K.I. Emelyanov

The paper discusses the masking of algebraic platforms, such as groups and groupoids. The idea of such a masking is transferred to a more complex platform — a 2-category.

Keywords: cryptography, masking of an algebraic platform, 2-category.

УДК 532.5.013.12

О РОЛИ НАСЛЕДСТВЕННОЙ СОСТАВЛЯЮЩЕЙ ГИДРОДИНАМИЧЕСКОЙ СИЛЫ ПРИ ДВИЖЕНИИ СФЕРИЧЕСКОГО ВИБРОРОБОТА В ВЯЗКОЙ ЖИДКОСТИ

О.С. Жучкова[1], А.Н. Нуриев[2]

1 *oszaharova@kpfu.ru*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

2 *corei7tesla3@gmail.com*; Казанский (Приволжский) федеральный университет, Институт математики и механики им. Н.И. Лобачевского

В работе проводится исследование вопросов о структуре гидродинамической силы сопротивления, возникающей при периодическом движении сферического виброробота в жидкости, и влиянии различных ее составляющих на процесс и эффективность движения. В том числе, выявляется роль наследственной силы сопротивления в динамике движения робота. Иследование проводится в рамках прямого численного моделирования с использованием программного пакета OpenFoam. Показано, что наследственная составляющая силы в случае конечных периодов движения дает вклад в суммарную силу, сравнимый с квазистационарным. Ее влияние существенно снижает эффективность рассматриваемого механизма движения для случая высокочастотных колебаний.

Ключевые слова: виброробот, гидродинамическое сопротивление, вязкая жидкость, самодвижущееся устройство, наследственные силы, силы присоединенных масс, квазистационарные силы.

Определение гидродинамических сил, возникающих при движении сферического тела в жидкости, относится к классическим проблемам гидромеханики. В данной работе она рассматривается применительно к задаче о поступательном дви-