

Применение топологически простых колец в криптографии

В. В. Тензина¹

В работе предлагается криптографическая схема шифрования на основе топологически простых коммутативным колец. Доказывается, что кольцо целых чисел топологически просто и на основе этого факта строится конкретная криптосхема.

Ключевые слова: топологически простое кольцо, топологически неприводимый модуль, криптографическая схема.

Везде считаем, что модули левые, топологические кольца и модули отделимые.

Топологическая простота кольца целых чисел относительно некоторой топологии

Кольцо без собственных замкнутых идеалов называется *топологически простым кольцом*.

В четвертом издании Днестровской тетради (см. [1], 1.10.), в которой изложены нерешённые проблемы теории колец и модулей, В.И. Арнаутым сформулирован следующий вопрос: существует ли в кольце целых чисел \mathbb{Z} такая неослабляемая топология, в которой \mathbb{Z} не содержит замкнутых идеалов. В данной работе даётся положительный ответ на этот вопрос.

В статье [2] строится неидеальная недискретная топология на кольце целых чисел. Дополнительно показывается, что можно построить несчётное число топологий такого типа. Такого типа топологии являются индуктивными, в дальнейшем для различных классов колец они рассматриваются в [3]. Мутылин в своей работе [4], используя похожую технику, строит кольцевую топологию на поле рациональных чисел. На основе этой топологии можно построить желаемую топологию, тем самым доказав

Теорема 1. *В кольце целых чисел \mathbb{Z} существует кольцевая топология, относительно которой \mathbb{Z} топологически просто.*

Следствие 1. *В кольце гауссовых чисел $\mathbb{Z}[i]$ существует такая топология, относительно которой $\mathbb{Z}[i]$ топологически просто.*

¹Тензина Виктория Васильевна — в.н.с. каф. теоретической информатики мех.-мат. ф-та МГУ, e-mail: viktoria.tenzina@math.msu.ru

Tenzina Viktoria Vasil'evna — PhD, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics.

Криптосхема на основе топологически простых коммутативных колец

Пусть R — топологически простое коммутативное кольцо с единицей. Например, кольцо целых чисел с индуктивной топологией. Выбираем в R конечное подмножество $\{x_i\}_{i=1}^N = X$. Это множество всех возможных сообщений, которые могут быть переданы и зашифрованы.

Для формирования параметров, отвечающих за шифрование и дешифрование, нам понадобится произвольный ненулевой элемент кольца $a \in R$ и произвольная окрестность нуля V_1 из R такая, что для любых различных элементов $x, y \in X$ подмножества $(x + V_1)$ и $(y + V_1)$ не пересекаются. Существование такой окрестности следует из делимости кольца и конечности множества X .

Стандартное обозначение того, что V_1 является окрестностью нуля: $V_1 \in \tau(R)$. Найдётся окрестность $V_2 \in \tau(R) : V_2 + V_2 \subset V_1$. В силу конечности X существует окрестность $V_3 \in \tau(R)$ такая, что $V_3x \subset V_2$ для любого $x \in X$.

Из-за того, что коммутативное кольцо R топологически просто и содержит единицу, найдётся элемент кольца b такой, что $ba \in 1 + V_3$. Пусть окрестность $V \in \tau(R)$ такова, что $bV \in V_2$.

Ключ шифрования (a, V) , ключ для расшифровки (b, V_1) .

Само **шифрование** устроено следующим образом. Пусть $x \in X$. Передаём $y = ax + v$, выбирая произвольный элемент v из V . Элемент v для данного x нестрого определен. В принципе v из V можно выбрать любым, принимая во внимание какие-то соображения. Например, чтобы передаваемые y были как можно более равновероятны.

Расшифровка: ищем x такое, чтобы $by \in x + V_1$. Оно такое единственное, так как

$$by = b(ax + v) = bax + bv \in (1 + V_3)x + bV \subseteq x + V_2 + V_2 \subset x + V_1.$$

Рассмотрим следующий **пример**. Пусть $R = \mathbb{Z}$ с индуктивной топологией $\tau(R) = \{U_n\}_{n=1}^\infty$. Пусть выбраны простые числа $\{p_i\}_{i=1}^\infty$ и натуральные $\{a_{ij}\}_{i \geq j \geq 1}$ так, что

$$\begin{aligned} p_1 < a_{11} < p_2 < a_{22} < a_{21} < p_3 < a_{33} < a_{32} < a_{31} < \\ < p_4 < a_{44} < a_{43} < a_{42} < a_{41} < \dots \end{aligned}$$

и подмножества $U_n = \{\sum_{k=n}^\infty t_k p_k : |t_k| \leq a_{kn}\}$ являются базой окрестностей нуля для некоторой топологии.

Такая топология существует (см. выше) и относительно неё \mathbb{Z} топологически просто. Заметим, что наборы $\{a_{ij}\}$ и $\{p_i\}$ могут быть различны и секретны.

Выбираем конечное множество X , например, $\{cs\}_{s=1}^N$, где $c \in \mathbb{N}$.

Фиксируем $a \in \mathbb{Z}$. Нам надо подобрать такое n , чтобы U_n можно было использовать в качестве V_1 . Затем находим V_1 , b и V по вышеописанному алгоритму.

Оценка сложности преобразований требует дальнейшего изучения. Эта сложность будет зависеть от конкретной выбранной топологии. Уже есть проблемы, чтобы конструктивно определить изначальную окрестность V_1 по множеству X , а при декодировании уметь определять какому подмножеству $\{x + V_1\}_{i=1}^N$ принадлежит by . Некоторые шаги построения V по V_1 понятны. Например, для вышеописанной индуктивной топологии в кольце целых чисел окрестность V_2 по V_1 определяется из соотношения $U_{n+1} + U_{n+1} \subseteq U_n$. Нужно более тщательное теоретическое исследование самой топологии. То что окрестности вообще-то содержат бесконечное число элементов, можно обойти, придя к конечным подмножествам, учитывая индуктивность построения самой базы вышеуказанной топологии.

Из окрестностей в самом кодировании и декодировании используются только V_1 и V . Фактически сама топология, топологическая простота R нам позволяет просто найти подходящие два конечных подмножества V_1 и V .

На самом деле сама идея такого шифрования чем-то похожа на криптосистемы, основанные на помехоустойчивых кодах. Например крипто-схема McEliece (см. [5]). То, что там некоторые определённые биты можно изменить на что угодно, похоже на прибавление элемента из заданной окрестности.

Какую-то подобную схему хотелось бы рассмотреть на основе топологически неприводимых модулей (в качестве X рассматриваем подмножество модуля). По крайней мере топология на топологически неприводимом модуле \mathbb{Z} над дискретным кольцом \mathbb{Z} (см. [6]) проще устроена (используется идея иррациональной обмотки тора). На самом деле при построении криптосхемы вместо коммутативного топологически простого кольца можно использовать коммутативное кольцо с единицей, являющееся топологически неприводимым модулем над собой как над дискретным кольцом.

Важно уметь на более менее понятных множествах эффективно вычислять: принадлежит ли заданный элемент данной окрестности, параметризуемой несколькими секретными параметрами? Например, окрестность кольца целых чисел, являющегося топологически неприводимым модулем, параметризуется маленьким $\varepsilon > 0$ (определяет интервал) и иррациональным числом (можно взять корень из натурального).

Дополнительно следует изучить возможности данной асимметричной схемы шифрования как криптосхемы с открытым ключом.

Рассмотрение таких схем стимулирует дальнейшее изучение свойств топологически неприводимых модулей, топологически простых колец и конструктивное построение топологий.

Список литературы

- [1] Сост. В.Т. Филиппов, В.К. Харченко, И.П. Шестаков, “Днестровская тетрадь. Нерешённые проблемы теории колец и модулей., 4-ое изд.”, 1993, 73 pp.
- [2] Hinrichs Lowell A., “Integer topologies”, *Proc. of the A.M.S.*, **15:6** (1964), 991-995
- [3] J.O. Kiltinen, “Inductive ring topologies”, *Trans. Amer. Math. Soc.*, **134** (1968), 149-169
- [4] Мутылин А. Ф., “Пример нетривиальной топологизации поля рациональных чисел. Полные локально ограниченные поля”, *Изв. АН СССР. Сер. матем.*, **30:4** (1966), 873-890
- [5] R. J. McEliece, “A Public-Key Cryptosystem Based On Algebraic Coding Theory”, 1978, 42-44
- [6] С.Т. Главацкий, А.В. Михалев, В.В. Тензина, “Топологический радикал Джекобсона колец, часть II”, *Фундамент. и прикл. матем.*, **17:1** (2011), 53-64

Cryptography based on topologically simple rings

Tenzina V.V.

The paper proves that the ring of integers is topologically simple with respect to a certain ring topology. Then we construct a cryptosystem based on commutative topologically simple rings.

Keywords: topologically simple ring, topologically irreducible module, cryptosystem

References

- [1] V. T. Filippov (ed.), V. K.Kharchenko (ed.), I. P. Shestakov (ed.), “The Dniester notebook. Unsolved problems in the theory of rings and modules. 4th ed.”, 1993 (In Russian), 73 pp.
- [2] Hinrichs Lowell A., “Integer topologies”, *Proc. of the A.M.S.*, **15:6** (1964), 991-995

- [3] J.O. Kiltinen, “Inductive ring topologies”, *Trans. Amer. Math. Soc.*, **134** (1968), 149-169
- [4] Mutylin A. F., “An example of a nontrivial topologization of the field of rational numbers. Complete locally bounded fields”, *Izv. Akad. Nauk SSSR, Ser. Mat.*, **30**:4 (1966), 873-890 (In Russian)
- [5] R. J. McEliece, “A Public-Key Cryptosystem Based On Algebraic Coding Theory”, 1978, 42-44
- [6] S. T. Glavatsky, A. V. Mikhalev, V. V. Tenzina, “The topological Jacobson radical of rings. II.”, *Fundam. Prikl. Mat.*, **17**:1 (2011), 53-64 (In Russian)