УДК 51-74

Исмагилова А.С.
Уфимский университет науки и технологий, Уфа

КРИПТОГРАФИЧЕСКИЕ АСПЕКТЫ ИЗОМОРФИЗМА ГРУПП ОБРАТИМЫХ ЭЛЕМЕНТОВ

Аннотация. В настоящей работе предложен подход к описанию процесса шифрования с использованием изоморфизма групп обратимых элементов ассоциативных колец с единицей. Показано, что такой подход позволяет моделировать преобразование данных, их разделение на логически независимые компоненты и применение различных режимов обработки − изоморфизма и антиизоморфизма. В качестве конкретной реализации рассмотрен пример на основе колец Z_3 и $M_2(Z_2)$, в котором центральный идемпотент определяет разложение кольца на прямую сумму и обеспечивает согласованное применение разных алгебраических преобразований к частям сообщения. Полученные конструкции могут быть использованы при построении гибридных криптографических схем, обеспечивающих дополнительные возможности для защиты информации.

Ключевые слова: открытый ключ, закрытый ключ, группа шифрования, группа расшифрования, изоморфизм.

Настоящее исследование основано на результатах автора, которые были опубликованы в работе [1]. Цель данной работы − описать криптографическую систему, где открытый текст представлен как элемент группы обратимых элементов ассоциативного кольца с единицей.

Пусть R и S − ассоциативные кольца с единицей, множества открытых/закрытых ключей. Разложения в прямую сумму $R = R_1 \oplus R_2$, $S = S_1 \oplus S_2$ могут соответствовать разделению данных на независимые компоненты, каждая из которых обрабатывается по-разному. Группы обратимых элементов $U(R)$ и $U(S)$ можно представить как группы шифрования/расшифрования. Пусть в R определена ортогональная система идемпотентов h_i, $\sum_{i=1}^{3} h_i = 1$, $Rh_iR = R$, в S − система g_j, $\sum_{j=1}^{2} g_j = 1$, $Sg_jS = S$. Ортогональные идемпотенты могут представлять собой разделение данных на части. Центральный идемпотент $e \in R$ определяет какая часть сообщения обрабатывается изоморфизмом $\theta_1 : R_1 \to S_1$, какая антиизоморфизмом $\theta_2 : R_2 \to S_2$. Процесс преобразования данных, защищенных с помощью одной криптографической схемы, в эквивалентные данные, защищенные другой схемой, можно описать как изоморфизм $\varphi : U(R) \to U(S)$.

Теорема. Если существует изоморфизм между группами обратимых элементов φ, то существует кольцевой изоморфизм θ_1, кольцевой

антиизоморфизм θ_2, такие, что $\varphi(A) = \theta_1(eA) + \theta_2\big((1-e)A\big)$, где $e \in R$, $A \in E(R)$, $E(R)$ − группа преобразований, порожденная элементом $1 + e_i x e_j$.

Теорему можно использовать не только в абстрактной математике, но и в современной криптографии. Приведем пример, реализующий данный результат.

Пусть кольцо R моделирует систему данных или шифрования, в которой информация может быть разделена на две независимые части ($R = R_1 \oplus R_2$). Здесь $R_1 = Z_3$ − кольцо вычетов по модулю 3 − содержит три элемента $\{0, 1, 2\}$ с операциями сложения и умножения по модулю 3. Например, это может быть цифровая подпись или короткий ключ. $R_2 = M_2(Z_2)$ − кольцо матриц размера 2×2 над Z_2, содержит $2^4 = 16$ элементов. К примеру, это кольцо может использоваться для сложных структур, таких как блоки шифруемого текста. Аналогично, $S = S_1 \oplus S_2$, где $S_1 = M_2(Z_2)$, $S_2 = Z_3$. То есть кольца R и S имеют одинаковые компоненты, но они расположены в обратном порядке. Если представить переход от R к S, то его можно рассматривать как переход между двумя различными криптографическими схемами.

Группы $U(R)$ и $U(S)$ − группы обратимых элементов над ассоциативными кольцами R и S, соответствуют обратимым операциям шифрования и расшифрования.

Группа $U(R)$ представляет собой совокупность обратимых преобразований, действующихй на парах − один элемент из Z_3, другой − из $M_2(Z_2)$:

$$U(R) = U(Z_3) \oplus U\big(M_2(Z_2)\big).$$

Здесь $U(Z_3) = \{1, 2\}$, поскольку эти два элемента имеют обратные по умножению в кольце вычетов Z_3. Группа невырожденных матриц размера 2×2 над Z_2 − $U\big(M_2(Z_2)\big)$ − содержит шесть элементов:

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

Аналогично, $\mathrm{U(S)} = \mathrm{U}\big(\mathrm{M_2(Z_2)}\big) \oplus \mathrm{U(Z_3)}$. Прямая сумма коммутативна с точностью до изоморфизма.

Существование изоморфизма $\varphi: U(R) \to U(S)$ групп обратимых элементов означает, что группы шифрования/расшифрования совпадают с точностью до перестановки частей. Иначе, обе системы допускают эквивалентные наборы.

Заметим, что кольца R_1 и S_1 не изоморфны как целые, но можно рассмотреть вложение − инъективный гомоморфизм из $\mathrm{Z_3}$ в $\mathrm{M_2(Z_2)}$. Вложение позволяет сохранить структуру части данных при отображении одного кольца в другое. Антиизоморфизм можно представить в виде транспонированной матрицы: $\theta_2(A) = A^T$. Это дополняет степень защиты, усложняя восстановление исходного сообщения без знания точного типа

отображения. В качестве центрального идемпотента выберем $e = (1,0) \in R$. Тогда $eA = (a, 0)$, $(1 - e)A = (0, b)$, где $A = (a, b) \in R$.

Приведенный пример показывает, как можно формализовать процесс шифрования данных, разделенных на части при помощи алгебраических преобразований. Такая схема может быть применена при построении гибридных криптосистем, где разные части сообщения защищаются разнвми методами, но при этом сохраняется согласованность между группами.

В перспективе планируется рассмотреть общие классы колец и исследовать устойчивость схем к различным типам криптоатак.

Список использованных источников:

1. Исмагилова, А.С. Изоморфизмы групп обратимых элементов ассоциативного кольца / А.С. Исмагилова // Вестник Башкирского университета. 2005. № 4, т. 10. С. 8–11.

Ismagilova A.S.
Ufa University of Science and Technology, Ufa

CRYPTOGRAPHIC ASPECTS OF ISOMORPHISM OF REVERSIBLE ELEMENT GROUPS

Abstract. In this paper, we propose an approach to describing the encryption process using the isomorphism of the groups of invertible elements of associative rings with identity. We show that this approach allows us to model data transformation, partitioning into logically independent components, and applying different processing modes, such as isomorphism and anti-isomorphism. As a specific implementation, we consider an example based on the rings Z_3 and $M_2(Z_2)$, where the central idempotent determines the decomposition of the ring into a direct sum and ensures the consistent application of different algebraic transformations to different parts of the message. The resulting designs can be used to build hybrid cryptographic schemes that provide additional information protection capabilities.

Keywords: public key, private key, encryption group, decryption group, and isomorphism.