УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА.
СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

2024, Т. 166, кн. 1
С. 52–57

ISSN 2541–7746 (Print)
ISSN 2500–2198 (Online)

ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 512.552

doi: 10.26907/2541-7746.2024.1.52-57

ПРОТОКОЛ ОБМЕНА КЛЮЧАМИ НАД КОЛЬЦОМ ФОРМАЛЬНЫХ МАТРИЦ $B_n(R, P)$

М.Ф. Насрутдинов

Казанский (Приволжский) федеральный университет, г. Казань, 420008, Россия

Аннотация

Рассмотрена возможность построения протокола обмена сообщениями над специальным классом формальных матриц $B_n(R, P)$. Показано, что такая конструкция позволяет получить протоколы обмена сообщениями, использовав произвольные ассоциативные кольца и идеалы над ними.

Ключевые слова: протокол обмена сообщениями, кольцо формальных матриц

Введение

Появление и развитие интернета привело к массовому применению криптографии для защиты информации, передаваемой по открытым каналам связи. Само по себе использование криптографии насчитывает несколько тысяч лет, но широкое применение математики для построения и анализа стойкости криптосистем началось с работы К. Шеннона "Математическая теория криптографии" [1], опубликованной в 1949 г.

Криптосистемы разделяют на симметричные, то есть системы, в которых для шифрования и расшифрования применен один и тот же криптографический ключ, и асимметричные (криптосистемы с открытым ключом). В асимметричных системах используются открытый ключ, который передается по открытому каналу, и закрытый ключ, который применяется для расшифровки. Начало асимметричным шифрам было положено в работе У. Диффи и М. Хеллмана [2], опубликованной в 1976 г. Методы шифрования с отрытым ключом применяются как для собственно шифрования, так и для обмена ключами по открытым каналам связи для дальнейшего применения симметричного шифрования, или как средство аутентификации пользователей.

Одной из первых реализаций идеи асимметричного шифрования была криптосистема RSA (см., например, [3]), базирующаяся на вычислительной сложности задачи факторизации больших чисел. С тех пор ведутся поиски подходящих математических объектов для построения асимметричных криптосистем.

В конце 1990-х гг. сформировалось направление исследований, которое можно назвать алгебраической криптографией (см., например, [4], [5]). Особенностью алгебраической криптографии является то, что криптографические протоколы строятся с использованием таких абстрактных алгебраических структур (платформ), как, например, некоммутативные группы, полугруппы, кольца. Исследо-

вания по алгебраической криптографии (так же как и по математической криптографии в целом) нацелены на построение тех или иных криптографических протоколов и на обоснование их криптостойкости, т.е. вычислительной сложности нахождения секретного ключа по тем или иным открытым данным (например, по открытому ключу).

В данной работе рассматривается протокол обмена ключами над кольцами специального вида, который мы обозначили через $B_n(R,P)$. Данная конструкция обобщает результаты [6] на более широкий класс колец.

1. Кольцо $B_n(R,P)$

В работе Г.М. Бергмана [7] рассматривалось кольцо эндоморфизмов абелевой группы $E_p = End(\mathbb{Z}_p \oplus \mathbb{Z}_{p^2})$, где p – простое число. Там же показано, что E_p состоит из p^5 элементов и E_p дает пример полулокального кольца, которое не вложимо в кольцо матриц над коммутативным кольцом.

В работах [8], [9] авторы рассмотрели свойства этих колец и построили над ними протокол обмена сообщениями. Преимуществом этого кольца является то, что его можно реализовать в виде колец матриц (точнее, кольцо формальных матриц) и все вычисления проводить сначала в кольце целых чисел, а потом брать результаты вычислений по подходящему модулю степени простого числа p.

В работе [10] приведена атака на этот протокол. Ключевым моментом в этой атаке было наличие большого количества обратимых элементов в E_p. Для кольца E_p их количество составляет $p^3(p-1)^2$, и вероятность того, что произвольный элемент будет обратимым, стремится к единице с ростом p.

В работе [6] конструкция кольца Бергмана была обобщена и рассматривалось кольцо $E_p^{(m)} = End(Z_p \oplus Z_{p^2} \oplus \ldots \oplus Z_{p^m})$. Авторы назвали его обобщенным кольцом Бергмана. В нем долю обратимых элементов можно сильно уменьшить, и был приведен протокол, для которого атака уже не применима. В [11] построен протокол обмена ключом между несколькими участниками (больше двух) на основе этого кольца. В [12] обсуждались вопросы атаки на построенный протокол.

В нашей совместно с С.Н. Трониным работе [13] конструкция кольца $E_p^{(m)}$ была обобщена следующим образом.

Пусть R – ассоциативное кольцо с единицей, P – двусторонний идеал R, $n \geq 2$ – натуральное число. Обозначим через

$$B_n(R,P) = \{(x_{ij}) | x_{ij} \in B_{ij}\} = \begin{pmatrix} R/P & R/P & \ldots & R/P \\ P/P^2 & R/P^2 & \ldots & R/P^2 \\ P^2/P^3 & P/P^3 & \ldots & R/P^3 \\ \ldots & \ldots & \ldots & \ldots \\ P^{n-1}/P^n & P^{n-2}/P^n & \ldots & R/P^n \end{pmatrix}$$

множество формальных матриц размера $n \times n$ ($B_{ij} = R/P^i$ при $i \leq j$, $B_{ij} = P^{i-j}/P^i$ при $i > j$) для любых $1 \leq i,\ j \leq n$.

Приведем для удобства необходимые сведения относительно строения кольца $B_n(R,P)$ из статьи [13].

1) На множестве $B_n(R,P)$ можно естественным образом определить операции сложения и умножения, превращающие его в ассоциативное кольцо с единицей [13, Теорема 1]. Это кольцо изоморфно кольцу эндоморфизмов правого R-модуля $R/P \oplus R/P^2 \oplus \ldots R/P^n$.

2) Центр кольца $B_n(R,P)$ состоит из матриц вида

$$\begin{pmatrix} z+P & 0 & \dots & 0 \\ 0 & z+P^2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & z+P^n \end{pmatrix},$$

где $z+P^n$ принадлежит центру кольца R/P^n [13, Теорема 4].

3) Матрица $A \in B_n(R,P)$ обратима тогда и только тогда, когда элементы на главной диагонали A_{ii} обратимы в R/P^i для всех $i = 1,2,\dots,n$ [13, Теорема 5].

Таким образом, мы получили целое семейство колец, которое может обладать лучшими характеристиками с точки зрения криптостойкости протокола обмена ключами.

2. Приложения в криптографии

Как сказано выше, в [9] был предложен протокол обмена сообщениями над кольцом E_p. В наших обозначениях это кольцо $B_2(\mathbb{Z}, p\mathbb{Z})$. Приведем описание этого протокола.

Пусть $f(X) = a_0 + a_1X + a_2X^2 + \dots a_nX^n \in \mathbb{Z}[X]$. Для элемента $M \in B_n(R,P)$ обозначим

$$f(M) = a_0E + a_1M + a_2M^2 + \dots a_nM^n,$$

где E – единичная матрица кольца $B_n(R,P)$.

Схема протокола описывается следующим образом:

1. Алиса и Боб публикуют открытые ключи $r, s \in \mathbb{N}$ и $M, N \in B_n(R,P)$.

2. Алиса и Боб выбирают закрытые ключи $f(X) \in \mathbb{Z}[X]$ и $g(X) \in \mathbb{Z}[X]$ соответственно.

3. Алиса вычисляет открытый ключ $P_A = f(M)^r N f(M)^s$ и посылает его Бобу.

4. Боб вычисляет открытый ключ $P_B = g(M)^r N g(M)^s$ и посылает его Алисе.

5. Алиса вычисляет $S_A = f(M)^r P_B f(M)^s$, Боб вычисляет $S_B = g(M)^r P_A g(M)^s$.

Так как элементы $f(M)^r$, $f(M)^s$, $g(M)^r$, $g(M)^s$ коммутируют, то $S_A = f(M)^r P_B f(M)^s = f(M)^r g(M)^r N g(M)^s f(M)^s = g(M)^r f(M)^r N f(M)^s g(M)^s = g(M)^r P_A g(M)^s = S_B$.

6. Таким образом, $S_A = S_B$ – общий ключ.

В [10] была предложена атака, основанная на следующей лемме.

Лемма 1. *Пусть $W_1, W_2 \in E_p$ такие, что*

$$W_1M = MW_1, \quad W_2M = MW_2, \quad P_BW_2 = W_1N.$$

Тогда

$$S_A = S_B = W_1P_AW_2.$$

Фактически для раскрытия ключа надо подобрать матрицы W_1 и W_2, коммутирующие с M, и W_2 должна быть обратимой. Подбор коммутирующих матриц сводятся к линейным уравнениям над $\mathbb{Z}_p$ и $\mathbb{Z}_{p^2}$, а обратимость матрицы при росте p получается практически автоматически в силу большой доли обратимых элементов в E_p.

При увеличении n доля обратимых элементов уменьшается. Так как строение обратимых элементов в кольце $B_n(R,P)$ известно, то мы можем достаточно просто оценивать этот параметр для каждого выбранного P.

В [6] протокол обмена ключами был усложнен следующим образом.

Обозначим через $C(B_n(R,P))$ центр кольца $B_n(R,P)$ (согласно [13] мы знаем его строение).

1. Алиса и Боб публикуют открытые ключи $M \in B_n(R,P)$, $N \in B_n(R,P) \setminus C(B_n(R,P))$.

2. Алиса выбирает закрытые ключи $f_1(X), f_2(x) \in C(B_n(R,P))[X]$ и $r,s \in \mathbb{N}$. Боб выбирает закрытые ключи $g_1(X), g_2(x) \in C(B_n(R,P))[X]$ и $u,v \in \mathbb{N}$.

3. Алиса вычисляет открытый ключ $P_A = f_1(M)^r N f_2(M)^s$ и посылает его Бобу.

4. Боб вычисляет открытый ключ $P_B = g_1(M)^u N g(M)^v$ и посылает его Алисе.

5. Алиса вычисляет $S_A = f_1(M)^r P_B f_2(M)^s$, Боб вычисляет $S_B = g_1(M)^u P_A g_2(M)^v$.

6. Элементы S_A и S_B равны, т. е. $S_A = S_B$. Таким образом, Алиса и Боб получают общий ключ.

В этом варианте протокола приведенная выше атака для кольца $B_n(\mathbb{Z}, p\mathbb{Z})$ уже не работает [6], но применима атака, основанная на применении теоремы Гамильтона – Кэли для коммутативных колец [12].

Заключение

Мы показали, что протоколы обмена ключами, приведенные в [8], [6], [11], допускают обобщения на кольцо вида $B_n(R,P)$. В качестве базового кольца R можно выбрать, например, кольцо многочленов над конечным полем или конечным коммутативным кольцом. С точки зрения приложений кольцо должно быть удобным для вычислений. Меняя базовое кольцо, мы потенциально можем получить протоколы с лучшими (с точки зрения криптостойкости) свойствами.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Литература

1. *Shannon C.E.* A mathematical theory of communication // Bell Syst. Tech. J. 1948. V. 27, No 3. P. 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

2. *Diffie W., Hellman M.E.* New directions in cryptography // IEEE Trans. Inf. Theory. 1976. V. 22, No 6. P. 644–654. https://doi.org/10.1109/TIT.1976.1055638.

3. *Ященко В.В.* Введение в криптографию. 4-е изд., доп. М.: МЦНМО, 2014. 347 с.

4. *Романьков В.А.* Алгебраическая криптография: монография. Омск: Изд-во Омск. гос. ун-та, 2013. 136 с.

5. *Myasnikov A., Shpilrain V., Ushakov A.* Non-Commutative Cryptography and Complexity of Group-Theoretic Problems. Ser.: Mathematical Surveys and Monographs. Vol. 177. Providence, RI: Am. Math. Soc., 2011. 385 p. https://doi.org/10.1090/surv/177.

6. *Climent J.-J., Navarro P.R., Tortosa L.* An extension of the noncommutative Bergman's ring with a large number of noninvertible elements // Appl. Algebra Eng., Commun. Comput. 2014. V. 25, No 5. P. 347–361. https://doi.org/10.1007/s00200-014-0231-6.

7. *Bergman G.M.* Some examples in PI ring theory // Isr. J. Math. 1974. V. 18, No 3. P. 257–277. https://doi.org/10.1007/BF02757282.

8. *Climent J.-J., Navarro P.R., Tortosa L.* On the arithmetic of the endomorphisms ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ // Appl. Algebra Eng., Commun. Comput. 2011. V. 22, No 2. P. 91–108. https://doi.org/10.1007/s00200-011-0138-4.

9. *Climent J.-J., Navarro P.R., Tortosa L.* Key exchange protocols over noncommutative rings. The case of End$(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ // Int. J. Comput. Math. 2012. V. 89, No 13–14. P. 1753–1763. https://doi.org/10.1080/00207160.2012.696105.

10. *Kamal A.A., Youssef A.M.* Cryptanalysis of a key exchange protocol based on the endomorphisms ring End$(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ // Appl. Algebra Eng., Commun. Comput. 2012. V. 23, No 3. P. 143–149. https://doi.org/10.1007/s00200-012-0170-z.

11. *Climent J.-J., López-Ramos J.A., Navarro P.R., Tortosa L.* Key agreement protocols for distributed secure multicast over the ring $E_p^{(m)}$ // WIT Trans. Inf. Commun. Technol. 2013. V. 45. P. 13–24. https://doi.org/10.2495/DATA130021.

12. *Zhang Y.* Cryptanalysis of a key exchange protocol based on the ring $E_p^{(m)}$ // Appl. Algebra Eng., Commun. Comput. 2018. V. 29, No 2. P. 103–112. https://doi.org/10.1007/s00200-017-0332-0.

13. *Nasrutdinov M.F., Tronin S.N.* On some class of formal matrix ring // Lobachevskii J. Math. 2022. V. 43, No 3. P. 677–681. https://doi.org/10.1134/S1995080222060269.

Поступила в редакцию 4.02.2024
Принята к публикации 6.02.2024

Насрутдинов Марат Фаритович, доцент кафедры компьютерной математики и информатики Института математики и механики им. Н.И. Лобачевского

Казанский (Приволжский) федеральный университет
ул. Кремлевская, д. 18, г. Казань, 420008, Россия
E-mail: *marat.nasrutdinov@kpfu.ru*

ISSN 2541–7746 (Print)
ISSN 2500–2198 (Online)

**UCHENYE ZAPISKI KAZANSKOGO UNIVERSITETA.
SERIYA FIZIKO-MATEMATICHESKIE NAUKI
(Proceedings of Kazan University. Physics and Mathematics Series)**

2024, vol. 166, no. 1, pp. 52–57

ORIGINAL ARTICLE

doi: 10.26907/2541-7746.2024.1.52-57

A Key Exchange Protocol Based on the Ring $B_n(R, P)$

M.F. Nasrutdinov

Kazan Federal University, Kazan, 420008 Russia
E-mail: *marat.nasrutdinov@kpfu.ru*

Received February 4, 2024; Accepted February 6, 2024

Abstract

A key exchange protocol over a special class of formal matrices $B_n(R, P)$ was proposed. The potential of this design for constructing key exchange protocols using suitable associative rings and ideals over them was shown.

Keywords: key exchange protocol, ring of formal matrices
Conflicts of Interest. The author declares no conflicts of interest.

References

1. Shannon C.E. A mathematical theory of communication. *Bell Syst. Tech. J.*, 1948, vol. 27, no. 3, pp. 379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.
2. Diffie W., Hellman M.E. New directions in cryptography. *IEEE Trans. Inf. Theory*, 1976, vol. 22, no. 6, pp. 644–654. https://doi.org/10.1109/TIT.1976.1055638.
3. Yashchenko V.V. *Vvedenie v kriptografiyu* [Introduction to Cryptography]. 4th enlarged ed. Moscow, MTsNMO, 2014. 347 p. (In Russian)
4. Roman'kov V.A. *Algebraicheskaya kriptografiya: monografiya* [Algebraic Cryptography: A Monograph]. Omsk, Izd. Omsk. Gos. Univ., 2013. 136 p. (In Russian)
5. Myasnikov A., Shpilrain V., Ushakov A. *Non-Commutative Cryptography and Complexity of Group-Theoretic Problems*. Ser.: Mathematical Surveys and Monographs. Vol. 177. Providence, RI, Am. Math. Soc., 2011. 385 p. https://doi.org/10.1090/surv/177.
6. Climent J.-J., Navarro P.R., Tortosa L. An extension of the noncommutative Bergman's ring with a large number of noninvertible elements. *Appl. Algebra Eng., Commun. Comput.*, 2014, vol. 25, no. 5, pp. 347–361. https: doi.org/10.1007/s00200-014-0231-6.
7. Bergman G.M. Some examples in PI ring theory. *Isr. J. Math.*, 1974, vol. 18, no. 3, pp. 257–277. https://doi.org/10.1007/BF02757282.
8. Climent J.-J., Navarro P.R., Tortosa L. On the arithmetic of the endomorphisms ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. *Appl. Algebra Eng., Commun. Comput.*, 2011, vol. 22, no. 2, pp. 91–108. https://doi.org/10.1007/s00200-011-0138-4.
9. Climent J.-J., Navarro P.R., Tortosa L. Key exchange protocols over noncommutative rings. The case of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. *Int. J. Comput. Math.*, 2012, vol. 89, nos. 13–14, pp. 1753–1763. https://doi.org/10.1080/00207160.2012.696105.
10. Kamal A.A., Youssef A.M. Cryptanalysis of a key exchange protocol based on the endomorphisms ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. *Appl. Algebra Eng., Commun. Comput.*, 2012, vol. 23, no. 3, pp. 143–149. https: doi.org/10.1007/s00200-012-0170-z.
11. Climent J.-J., López-Ramos J.A., Navarro P.R., Tortosa L. Key agreement protocols for distributed secure multicast over the ring $E_p^{(m)}$. *WIT Trans. Inf. Commun. Technol.*, 2013, vol. 45, pp. 13–24. https://doi.org/10.2495/DATA130021.
12. Zhang Y. Cryptanalysis of a key exchange protocol based on the ring $E_p^{(m)}$. *Appl. Algebra Eng., Commun. Comput.*, 2018., vol. 29, no. 2, pp. 103–112. https://doi.org/10.1007/s00200-017-0332-0.
13. Nasrutdinov M.F., Tronin S.N. On some class of formal matrix ring. *Lobachevskii J. Math.*, 2022, vol. 43, no. 3, pp. 677–681. https://doi.org/10.1134/S1995080222060269.

⟨ ***Для цитирования*:** *Насрутдинов М.Ф.* Протокол обмена ключами над кольцом формальных матриц $B_n(R,P)$ // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. 2024. Т. 166, кн. 1. С. 52–57. URL: https//doi.org/10.26907/2541-7746.2024.1.52-57. ⟩

⟨ ***For citation*:** Nasrutdinov M.F. A key exchange protocol based on the ring $B_n(R,P)$. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2024, vol. 166, no. 1, pp. 52–57.
URL: https//doi.org/10.26907/2541-7746.2024.1.52-57. (In Russian) ⟩