УДК 512.548.7, 512.554

В. М. Буняк[1]
Г. В. Шелепало (Крайнічук)[2]

АНАЛІЗ КРИПТОСХЕМИ НАД КВАЗІГРУПОВИМИ КІЛЬЦЯМИ

[1,2] Вінницький національний технічний університет;

Анотація

Вивчено метод побудови криптосхеми на основі автоморфізмів квазігруп, описано алгоритм криптосхеми над квазігруповими кільцями.

Ключові слова: квазігрупа, лупа, кільце, градуйоване кільце, мультиплікативний базис, криптосхема, автоморфізм, централізатор, відкритий ключ, криптограма, криптопротокол.

Abstract

The method of constructing a cryptoschema based on automorphisms of quasigroups is studied, the algorithm of cryptoschema over quasigroup rings is described.

Keywords: quasigroup, loop, ring, graduated ring, multiplicative basis, cryptoscheme, automorphism, centralizer, public key, cryptogram, cryptoprotocol.

Вступ

Ідентифікація дозволяє суб'єктові (користувачеві, процесу, що діє від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я). За допомогою аутентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає.

У[4] рядом авторів була проаналізована роль квазігрупових кілець в криптографії для ідентифікації двох учасників. Описані множини алгебричних структур [5] розширюють шифрування відкритих ключів у вигляді набору автоморфізмів, що підходять для визначених криптосхем.

Метою роботи є демонстрація методу побудови криптосхеми над квазігруповими кільцями.

Допоміжні поняття для результатів дослідження

На сьогодні теорія квазігруп і луп має широке застосування в різних галузях науки, зокрема і в криптографії (шифрування, побудова кодів). *Квазігрупою* [1] називається групоїд $(Q, \cdot)$, в якому для довільних елементів a, b з множини Q кожне з рівнянь $x \cdot a = b$ і $a \cdot y = b$ має єдиний розв'язок. Кількість елементів носія називається *порядком* квазігрупи. Обчислення числа квазігруп (латинських квадратів) порядку n − відома складна комбінаторна задача. Кількість скінченних квазігруп з точністю до ізоморфізму вдалося порахувати до 11-го порядку [3]:

$$q_{11} = 194645739166892496679102304393757829902 5 \approx e^{e^{4,5}} > 19 \cdot 10^{39}.$$

Така велика кількість квазігруп дає можливість сучасним алгоритмам бути криптостійкими, швидкодійними та водночас більш захищеними від зламу [6].

Криптограма – це схований, зашифрований тайнопис, що розкривається за допомогою набору встановлених правил, з відтворенням схованого запису для прочитання відправленої інформації. Сучасні криптографічні алгоритми шифрування поділяють на симетричні (з одним ключем для шифрування та дешифрування) та асиметричні (з відкритим ключем та секретним ключем шифрування та дешифрування відповідно). Відкритий ключ, це той, який дозволяється передавати по відкритих каналах зв'язку. Секретний – ключ, що має зберігатися в таємниці, або передаватися з використанням закритого каналу зв'язку. Ще в криптосхемі застосовується сеансовий ключ – це ключ, що використовується під час сеансу обміну повідомленнями для захисту каналу зв'язку.

Математична складова для результатів дослідження

Для кращого розуміння демонстрації методу побудови криптосхеми наведемо основні поняття та означення, які використовуються для дослідження.

Групоїд – непорожня множина із заданою бінарної операцією. Нехай $(G, \cdot)$ – групоїд, a - деякий елемент з G. Розглянемо відображення $L(a) : G \to G$, $R(a): G \to G$ для будь-якого $a \in G$. Визначимо їх таким чином: $xL(a) = x \cdot a$, $xR(a) = a \cdot x$ для будь-яких $x \in G$. Квазігруппа – такий групоїд $(G, \cdot)$, що відображення $L(a)$, $R(a)$ є бієкція для будь-якого $a \in G$. Групоїд $(G, \cdot)$ називається *лупою*, якщо $(G, \cdot)$ є квазігрупою з одиницею. Для будь-якого елементу a лупи $(G, \cdot)$ визначимо елементи a^{λ} і a^{ρ} умовами $a^{\lambda} \cdot a = 1$ і $a \cdot a^{\rho} = 1$. Кільце – сукупність елементів довільної природи, для яких визначені дві бінарні операції – додавання (+) і множення (позначається ·).

Нехай K – асоціативне кільце з одиницею, L – лупа або квазігрупа. Розглянемо множину KL (*квазігрупове (лупове) кільце*), що складається з усіх сум виду $\sum_{l \in L} \alpha_l \cdot l$ ($\alpha_l \in K$), в яких скінченна кількість елементів α_l відмінних від нуля. Два елементи $a, b \in KL$ рівні тоді і тільки тоді, коли $\alpha_l = \beta_l$ для всіх $l \in L$. На множині KL визначені операції додавання і множення в такий спосіб: якщо $a = \sum_{l \in L} \alpha_l \cdot l$ і $b = \sum_{l \in L} \beta_l \cdot l$ – елементи KL, то $a+b = \sum_{l \in L} (\alpha_l + \beta_l) \cdot l$, $ab = \sum_{l \in L} (\sum_{m,\, h \in L:\, mh = l} \alpha_m \beta_m)\, l$. Відносно цих операцій множина KL є неасоціативним кільцем з одиницею. Зручно ототожнити $l \in L$ з елементом $1 \cdot l \in KL$, а $\alpha \in K$ – з елементом $\alpha \cdot e$, де e – одиниця лупи, тоді K і L є підмножинами в KL.

Якщо R – асоціативне кільце з одиницею $1 \in R$, то розглянемо групу G в мультипликативному записі з нейтральним елементом $e \in G$. Кільце R називається *G-градуйованим*, якщо існує така сім'я $R_\sigma : \sigma \in G$ адитивних підгруп R_σ адитивної групи R, що $R = \bigoplus_{\sigma \in G} R_\sigma$, $R_\sigma R_\tau \subseteq R_{\sigma\tau}$ для всіх $\sigma, \tau \in G$. *Строго градуйованим* називається G-градуйоване кільце R, для якого виконується рівність $R_\sigma R_\tau = R_{\sigma\tau}$ для всіх $\sigma, \tau \in G$. Однорідним ступеня σ називається елемент $x \in R_\sigma$. Множину оборотних за множенням елементів в кільці R позначають $U(R)$. Мультиплікативний базисом алгебри R називається такий її базис B, що $B \cup \{0\}$ замкнуте відносно множення. Аннулятор (правий/лівий) множини M в кільці R – множина всіх елементів, таких, що для будь-якого r і будь-якого $x \in M$ виконується рівність $xr = 0$.

Побудова криптосхеми

В [2] розглядаються автоморфізми (ізоморфне відображення множини з даною системою операцій і відображень на себе) лупового кільця KL. З автоморфізмів $\varphi \in \mathrm{Aut(K)}$ і $\psi \in Aut(L)$ складається $\chi \in Aut(KL)$ за таким правилом: для будь-якого $h = a_{l1} l_1 + \cdots + a_{ln} l_n, h \in KL$, за означенням визначається $\chi(h) = \varphi(a_{l1})\psi(l_1) + \cdots + \varphi(a_{l_n})\psi(l_n)$. Таким чином, якщо відома структура груп автоморфізмів $Aut\,(K)$ і $Aut\,(L)$ окремо, тобто є можливість будувати досить багато автоморфізмів з $Aut\,(KL)$.

Нехай тепер R - кільце, градуйоване скінченною групою G. Тоді, як доведено в лемі 2 [4] R_e – підкільце в R, і, як випливає з наслідку 3 [4], підгрупа R_σ буде R_e-бімодуль для будь-якого $\sigma \in G$. Якщо описана група автоморфізмів для підкільця R_e, то, в загальному випадку, зафіксувавши $\varphi \in Aut(R_e)$, однозначно визначити автоморфізм для всього R не можна. Справді, для цього необхідно поширити дію φ на модулі $R\sigma$ і таким чином отримати $\chi \in Aut(R)$. Для цього необхідно, щоб $\chi(r_{\sigma 1} r_{\sigma 2}) = \chi(r_{\sigma 1})\chi(r_{\sigma 2})$ для $r_{\sigma 1} \in R_{\sigma 1}, r_{\sigma 2} \in R_{\sigma 2}, r_{\sigma 1} r_2 \in R_{\sigma 1 \sigma 2}$.

Але якщо у кільця R існує мультиплікативний базис B над R_e, то $R = R_e B$. Тому автоморфізм φ природньо продовжується до автоморфізму χ всього кільця R. У силу того, що B утворює напівгрупу за множенням, задаємо $\psi \in Aut\,(B)$. Цей автоморфізм буде змінювати сам мультиплікативний базис. Але навіть, якщо вибрти інший мультиплікативний базис, то отримаємо, взагалі кажучи, вже нові структури для шифрування зі своїми автоморфізмами. Це розширює множину відповідних для криптосхеми алгебричних структур. Для даного випадку, алгоритм криптосхеми передбачає два учасники: наприклад Катя (Учасник A) і Рома (Учасник B).

Учасник A:

1) Вибирає квазігрупове кільце R, таке, що групи автоморфізмів $Aut(B)$ і $Aut(R_e)$ некомутативні. Передбачається, що групи $Aut(B)$ і $Aut(R_e)$ досить багаті на елементи, що не комутують, великого порядку з нетривіальними централізаторами великого порядку. Покладемо і $|Aut(B)| \geq t_1$, $|Aut(R_e)| \geq t_2$. Тут і далі і t_i - параметри безпеки, які за припущенням експоненціально залежать від порядку градуйованого кільця R.

Фіксує градуювання і цей базис (в разі, якщо кільце допускає кілька різних базисів) з урахуванням перерахованих вище умов. Ця інформація оголошується по відкритому каналу. Позначимо базис через B, а групу, по якій градуйована кільце, - через G, тоді загальновідомі (R,G,B).

2) Задає автоморфізм $\sigma \in Aut(R_e)$ так, щоб порядок $|\sigma| > t_3$, причому σ повинен мати нетривіальний централізатор і $|C(\sigma) \setminus \langle\sigma\rangle| \geq t_4$.

Будує автоморфізм $\eta \in Aut(B)$ так, щоб $|\eta| \geq t_5$, причому η повинен мати нетривіальний централізатор і $|C(\eta) \setminus \langle\eta\rangle| \geq t_6$.

3) Випадково обирає автоморфізм $\tau \in |C(\sigma) \setminus \langle\sigma\rangle|$.

4) Випадково вибирає $\omega \in C(\eta) \setminus \langle\eta\rangle$.

5) За τ і ω будує секретний ключ, тобто автоморфізм $\phi \in Aut(R)$ так: для будь-якого $h \in R$ виду $h = ab_1 b_1 + \ldots + a_{b_n} b_n$, де $a_{b_1}, \cdots, a_{b_n} \in R_e$, вважає, що $\varphi(h) = \tau(a_{b_1})\,\omega(b_1) + \cdots + \tau(a_{b_n})\,\omega(b_n)$.

6) Обирає елементи $a \in R$, $x \in R$ з нульовими лівими ануляторами. Це умова необхідна для подальшого розшифрування.

7) Обчислює $\varphi(x)$ і $\varphi(a)$. Таким чином, відкритим ключем учасника A є $(\sigma, \eta, x, \phi(x), a, \phi(a))$.

Відзначимо, що при параметрах безпеки t_3, t_4, t_5, t_6, автоморфізмів, придатних для відкритого ключа, є досить багато. Сформований відкритий ключ Катя передає Ромі відкритим каналом.

Участник B:

1) Вибирає натуральні числа i, j, k, l.

2) Використовуючи відкритий ключ учасника A, отримує пари автоморфізмів (σ^i, η^j), (σ^k, η^l) і за ними будує автоморфізм $\psi, \chi \in Aut(KL)$ таким же способом, як і учасник A. Тобто для будь-якого $h \in KL$ виду $h = a_{l_1} l_1 + \cdots + a_{l_n} l_n$ вважає, що

$$\psi(h) == \sigma^i(a_{l_1})\eta^j(l_1) + \cdots + \sigma^i(a_{l_n})\eta^j(l_n), \chi(h) = \sigma^k(a_{l_1})\eta^l(l_1) + \cdots + \sigma^k(a_{l_n})\eta^l(l_n).$$

Автоморфізми ψ, χ будемо називати сеансовими ключами.

3) Обчислює $\chi(a) \cdot \psi(x)$ та обчислює $\chi(\phi(a)) \cdot \psi(\phi(x))$. Оскільки елементи a і x були обрані з нульовим лівим анулятором, то і у цього добутку буде нульовий лівий анулятор.

4) Записує вихідний текст, який треба передати, у вигляді $m \in R$ і обчислює $m \cdot [\chi(\varphi(a)) \cdot \psi(\varphi(x))]$. Вихідний текст можна розбити на блоки і кожен зашифрувати окремо з різними секретними ключами.

5) Відправляє для A криптограму $(\chi(a) \cdot \psi(x), m \cdot [\chi\phi(a)) \cdot \psi\phi(x)])$.

Отриману криптограму розшифровує Учасник A:

1) Використовуючи секретний автоморфізм φ, обчислює $q = \varphi(\chi(a) \cdot \psi(x))$.

2) Розшифровує надісланий текст, користуючись тим, що χ, ψ і φ комутують. Таким чином, учасник A знає $h = m \cdot [\chi(\varphi(a)) \cdot \psi(\varphi(x))]$ і $\varphi(\chi(a) \cdot \psi(x))$. Для розшифрування повідомлення m досить розв'язати лінійну систему $m \cdot q = h$ з коефіцієнтами з кільця R_e, яка завжди має єдиний розв'язок, тому що автоморфізми τ і σ, а також ω і η попарно комутують між собою. Внаслідок комутування на їх основі утворюються автоморфізми φ і ψ, φ і χ. Як результат цього $\chi(\varphi(a)) \cdot \psi(\varphi(x)) = \varphi\chi(a) \cdot \psi(x) = q$. Крім того, елемент $\chi(\varphi(a)) \cdot \psi(\varphi(x))$ обраний з нульовим лівим анулятором. Тому система рівнянь $m \cdot q = h$ з коефіцієнтами з кільця R_e має єдиний розв'язок.

Висновки

На сьогодні маємо підвищений інтерес до вивчення квазігруп та латинських квадратів, тому що розробка методів [6] шифрування та дешифрування даних з використанням квазігруп, луп, латинських квадратів, кубів та гіперкубів дасть можливість значно підвищити надійність передачі даних незахищеними каналами. Проаналізована побудова криптосхеми за допомогою автоморфізмів квазігруп, яка буде використана в роботі криптопротоколу для ідентифікації користувачів. А сам криптопротокол може бути впроваджений для захисту інформації від втручання кіберзлочинців.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Белоусов В.Д. Основы теории квазигрупп и лупп/ М.: Наука, − 1967г. − 223с.
2. Грибов А.В. Построение алгебраической криптосистемы над квазигрупповым кольцом / А.-В. Грибов, П. А. Золотых, А. В. Михалёв // Математические вопросы криптографии. 2010. Т. 1. № 4. С. 23–33.
3. McKay B. D. and Wanless I. M. On the number of Latin Squares // Ann. Combin. − 2005. − No. 9. − P. 335-344.
4. Марков В. Т. Квазигруппы и кольца в кодировании и построении криптосхем. / В. Т. Марков, А. В. Михалёв, А. В. Грибов [та ін.] // Прикладная дискретная математика. Мат. методы криптографии. – 2012. – №4(18). — 31-52 с.
5. Марков В. Т. Неассоциативные алгебраические структуры в криптографии и кодировании. / В.-Т. Марков, А. В. Михалёв, А. А. Нечаев // Фундаментальная и прикладная математика. – 2016. – №4. – 99-123 с.
6. Cryptographic Primitives with Quasigroup Transformations. / A. Mileva // The Faculty of Natural Science Library. – 2009. – 73-126 с.

Буняк Віталій Михайлович — студент групи 2БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vetalbunjak@gmail.com

Науковий керівник: ***Шелепало (Крайнічук) Галина Василівна*** — кандидат фізико-математичних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Buniak Vitalii M. — Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : vetalbunjak@gmail.com

Supervisor: ***Shelepalo (Krainichuk) Halyna V.*** — Candidate of Physical and Mathematical Sciences, Associate Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia