

ПРО ДЕЯКІ КВАЗІГРУПОВІ ТОТОЖНОСТІ МІНІМАЛЬНОЇ ДОВЖИНИ У ШИФРУВАННІ

Вінницький національний технічний університет

Анотація. В роботі описано квазігрупові тотожності мінімальної довжини, що найчастіше застосовуються у шифруванні та різноманітних криптосистемах. Знайдено властивість квазігрупи, яка має найменшу вагу (в GE) у відповідному алгоритмі потокового шифрування для LW-криптографії.

Ключові слова: квазігрупа, тотожність, симетрія, потокове шифрування, LW-криптографія, кібербезпека.

Анотація. In the theses, quasigroup identities of minimal length, which are most often used in encryption and various cryptosystems, are described. A property of a quasigroup that has the smallest weight (in GE) in the corresponding stream encryption algorithm for LW cryptography is found.

Ключові слова: quasigroup, identity, symmetry, stream encryption, LW cryptography, cybersecurity.

Вступ

Ідентифікація квазігрупових тотожностей мінімальної довжини має особливе значення. Коротші тотожності не тільки забезпечують більш стисле зображення визначальних властивостей квазігрупи, але також пропонують розуміння основних компонентів, які відрізняють один клас квазігруп від іншого. Часто виникає питання про утворення квазігруп з визначеними властивостями особливо це стосується шифрування. Оптимальними методами для такого створення є алгебричні методи, що передбачають попереднє вивчення конкретних класів квазігруп. Найбільш вивченими серед усіх таких класів є многовиди, тобто класи квазігруп, що визначаються за допомогою тотожностей.

Вважають, що тотожність має мінімальну довжину, якщо в ній кількість появ кожної предметної змінної найменша. Тотожність має тип $(m; n)$, якщо вона має дві предметних змінних, кожна з яких має відповідну кількість появ, а саме перша змінна — m появ, друга змінна — n появ. У [1] показано, що кожна скінченна квазігрупа $(Q; \cdot)$ задовольняє деяку тотожність типу $(m; 2)$ для деякого m . З цього твердження випливає доцільність вивчення многовидів квазігруп, що визначаються тотожностями типу $(m; 2)$. Описані множини тотожностей квазігруп типу $(3; 2)$, основною властивістю яких є взаємна-ортогональність парастрофів, що найкраще відходить для різних видів шифрування. Більш точно, досліджено, що відповідно до парастрофної рівносильності таких класів існує сім, які Білоусов В.Д. продемонстрував у вигляді тотожностей мінімальної довжини типу $(3; 2)$ та типу $(3; 3)$. Повну класифікацію квазігрупових тотожностей мінімальної довжини з точністю до парастрофно-первинної рівносильності здійснено в [2].

Проте, як виявилось, що у криптографії широко застосовуються навіть уже квазігрупові тотожності типу $(2; 2)$. А саме, шифр Edon-R [3] будується на основі квазігрупової тотожності:

$$(x \cdot y) \cdot y = x \quad (1)$$

Крім цього, інша квазігрупова тотожність найменшої довжини типу $(2; 2)$ може використовуватися для методу шифрування Edon-L, зокрема

$$x \cdot (x \cdot y) = y \quad (2)$$

Мінімальні квазігрупові тотожності типу $(3; 2)$ теж мають влучне застосування в шифруванні. А саме, перший закон Білоусова, задовольняє тотожність: $x \cdot (x \cdot xy) = y$, на якій описаний алгоритм шифру Edon-80 [4]. Крім того, Марковський С. розширив застосування квазігрупової тотожності мінімальної довжини типу $(m; 2)$, яка є узагальненням першого закону Білоусова:

$$\underbrace{x \cdot (\dots (x \cdot (x \cdot y)) \dots)}_m = y, \quad \dots ((y \cdot \underbrace{x \cdot x}_m) \cdot \dots) \cdot x = y.$$

Квазігрупи, що задовольняють ці дві тотожності називаються Шапелес квазігрупи (Shapeless quasigroups). Саме ці тотожності лягли в основу багатьох різноманітних криптосистем [4,5].

Метою роботи є покращення методу потокового шифрування на основі тотожностей мінімальної довжини з відповідними властивостями квазігруп.

Результати дослідження

Квазігрупою [1] називається універсальна алгебра $(Q; \cdot, /, \backslash)$ сигнатури $(2; 2; 2)$, що задовольняє такі тотожності для будь-яких $x, y \in Q$

$$x \cdot (x \backslash y) = y, \quad (y / x) \cdot x = y, \quad x \backslash (x \cdot y) = y, \quad (3)$$

де Q — бінарний групоїд, з визначеним на ньому набором бінарних операцій $(\cdot, /, \backslash)$, де символом $(/)$ позначають ліве ділення головної операції $(\cdot)$, а символом $(\backslash)$ — праве ділення головної операції $(\cdot)$.

Також, інші означення квазігрупи [2] доповнюють дане означення за допомогою тотожностей:

$$(y \cdot x) / x = y, \quad x / (y \backslash x) = y, \quad (x / y) \backslash x = y. \quad (4)$$

З властивостей (3) і (4) випливає, що операціям на квазігрупах невластиве поняття асоціативності, що відрізняє їх від інших алгебричних структур, таких як групи, де операція асоціативна.

Квазігрупа, яка має двосторонній одиничний елемент, називається лупою. Лупа — це квазігрупа для якої існує такий елемент e , що виконується така тотожність $ae = e \cdot a = a$ для $\forall a \in Q$.

Дві тотожності вважаються парастрофно рівносильними, якщо одну можна отримати з іншої за допомогою обмеженої кількості застосувань рівностей: $(x \backslash y) \cdot y = x$, $x \cdot (x / y) = y$ та перейменуванням змінних операції та предметних змінних.

З точністю до парастрофної рівносильності здійснено класифікацію тотожностей мінімальної довжини [2] відповідно до якої, існує 6 класів квазігруп:

- комутативні квазігрупи, задовольняють тотожність:

$$x \cdot y = y \cdot x; \quad (5)$$

- право-симетричні квазігрупи, що задовольняють тотожність (1);
- ліво-симетричні квазігрупи, що задовольняють тотожність (2);
- тотально-симетричні, що задовольняють одночасно (1) і (5), або (2) і (5);
- напів-симетричні, що задовольняють тотожність $x \cdot (y \cdot x) = y$ або $(y \cdot x) \cdot y = x$;
- асиметричні, в яких не виконуються тотожності типу $(2; 2)$.

Висновки

Встановлено, що найменшу вагу (в GE) для потокового шифрування мають тотально-симетричні квазігрупи. Квазігрупа називається тотально-симетричною, якщо всі її оборотні операції збігаються, тобто латинський квадрат один для многовида таких квазігруп. Оборотною називається операція, якщо для неї існує обернений елемент, що є важливою ознакою для шифрування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Keedwell A. D., Denes J. Latin Squares and their Applications // North Holland: Elsevier B.V. – 2015. – 455 p.
2. Шелепало Г. В. Класифікація квазігрупових функцій них рівнянь і тотожностей мінімальної довжини: дис. ... канд. фіз.-мат. наук: 01.01.06. Хмельницький. – 2019. – 191с.
3. Gligorosko D., Markovski S., Kocarev L., Edon-R, An Infinite Family of Cryptographic Hash Functions // International Journal of Network Security. – 2009. – Vol.8, No.3. – P.293-300.
4. D. Gligoroski, S. Markovski, S.J. Knapskog. On periods of Edon-(2m, 2k) family of stream ciphers // The State of the Art of Stream Ciphers, Workshop Record, SASC 2006. – Leuven, Belgium. – 2006. – pp.1-8.
5. Xiaomei Wang, Yunqing Xu Modification of Edon80 to Resist the Key Recovery Attack // First Internat. Conf. on Information Science and Electronic Technology (ISET 2015). – 2015. DOI:10.2991/iset-15.2015.2.

Крайнічук (Шелепало) Галина Василівна – к.фіз.-мат.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, Україна, email: hv.shelepalo@vntu.edu.ua

Корінний Олександр Олегович – студент групи 1БКС-21б, Вінницький національний технічний університет, Вінниця, Україна, email: olexandr.korinnyi@gmail.com

Krainichuk (Shelepalo) Halyna Vasylyivna – Candidate of Physical and Mathematical Sciences, Docent of the Department of Information Protection, Vinnytsia National Technical University, e-mail: hv.shelepalo@vntu.edu.ua

Korinnyi Oleksandr Olehovich – student of group 1BCS-21b, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: olexandr.korinnyi@gmail.com