УДК 004.056

В.В. Лавров[1]
Г. В. Шелепало (Крайнічук)[2]

АНАЛІЗ АТАК НА КРИПТОСИСТЕМУ БЛОКОВОГО ШИФРУ НА ОСНОВІ КВАЗІГРУП

[1,2] Вінницький національний технічний університет

Анотація

Дана робота оцінює стійкість та захищеність криптопротоколу від реалізації атак націлених на криптограму, вихідні тексти та сеансові ключі, які є автоморфізмами блокового шифру, побудованого на квазігрупах.

Ключові слова: квазігрупа, лупа, кільце, автоморфізм, криптограма, блоковий шифр, атака на криптограму, атака з вихідним текстом, атака на сеансовий ключ.

Abstract

This paper evaluates the stability and security of the cryptoprotocol from the implementation of attacks aimed at cryptogram, source code and session keys, which are automorphisms of a block cipher built on quasigroups.

Keywords: quasigroup, loop, ring, automorphism, cryptogram, block cipher, attack, attack on cryptogram, attack with source text, attack on session key.

Вступ

У літературі [3] виділяють різні способи захисту інформації, одним із них є шифрування. Захист даних за допомогою шифрування – це можливість розв'язати проблеми безпеки [1]. Зашифровані дані стають доступними тільки тим, хто знає, яким методом їх можна розшифрувати, і тому викрадення зашифрованих даних є абсолютно безглуздим для тих, хто використовує несанкціонований доступ.

Як алгебраїчна структура, квазігрупа є продуктом XX століття, однак, її комбінаторний аналог – латинський квадрат застосовується, набагато довше, ще з часів античності, для кодування текстів [3]. У криптографії використання квазігрупи забезпечують цікавий підхід до проектування певних методів шифрування тому що квазігрупи дають можливість підвищеної безпеки та високої швидкості сучасних криптопротоколів.

Метою роботи є перевірка атак з криптограмою, з вибраним вихідним текстом, а також на сеансові ключі, які є автоморфізмами квазігрупового кільця.

Результати дослідження

На сьогоднішній день розроблено багато стійких блокових шифрів. Практично всі алгоритми використовують для перетворень певний набір бієктивних математичних перетворень, які одночасно є оборотними [3]. Характерною особливістю блокових алгоритмів є той факт, що в ході своєї роботи вони виробляють перетворення блоку вхідної інформації фіксованої довжини і отримують результуючий блок того ж обсягу, але недоступний для прочитання сторонніми особами, що не володіють ключем. У дослідженні проаналізовано декілька найбільш можливих атак на криптопротокол. Основні означення понять та математичний апарат для розуміння результатів дослідження сформований та описаний в [2].

Розглянемо таку задачу. Нехай R – деяка алгебрична структура, A – деяка підмножина автоморфізмів $Aut\ R$, α – випадково обраний елемент з A. Припустимо, що відома деяка множина пар $(x_i, \alpha(x_i))$, $i = 1, \dots, n$ де $x_1 \in R$. Потрібно знайти автоморфізм $\alpha' \in A$, такий, що $\alpha`(x_i) = \alpha(x_i)$ для всіх $i = 1, \dots, n$. Позначимо цю задачу як $\Omega_n(A, R)$.

Зауважимо, що при відсутності істотньої інформації про множини A та R задача $\Omega_n(A, R)$ є обчислювально-складною, оскільки вона має розв'язок тільки повним перебором всіх елементів множини A і перевіркою умови $\alpha`(x_i) = \alpha(x_i)$, $i = 1, \dots, n$, для кожного обраного $\alpha` \in A$.

Атака тільки з криптограмою. Нехай криптоаналітик має доступ до відкритого ключа учасника A і до криптограми. Перед ним поставлена така задача: за відомими парам $(a, \epsilon(a)), (x, \epsilon(x))$ знайти такий

$\alpha \in Aut(R)$, з автоморфізмами $(\eta'\sigma')$, що $\sigma(a), = \alpha(a), \epsilon(x) = \alpha(x)$. Також необхідно щоб $\sigma' \in C(\sigma)\backslash\langle\sigma\rangle$ а $\eta' \in C(\eta) \setminus \langle\eta\rangle$.

Побудуємо α. Покладемо $\alpha(a) \coloneqq \varphi(a), a(x) \coloneqq \varphi(x)$. Таким чином, визначені $\alpha(ax) = \alpha(a) * \alpha(x) \coloneqq \varphi(a) * \varphi(x)$ та $\alpha(xa) = \alpha(x) * \alpha(a) \coloneqq \varphi(x) * \varphi(a)$. Але довизначити α на елемент $\chi(a) * \phi(x)$ можна лише перебором його образу з перевіркою того, що $\sigma' \in C(\sigma)\backslash\langle\sigma\rangle$а $\eta' \in C(\eta)\backslash\langle\eta\rangle$. Це не легше ніж перебір всіх автоморфізмів створених парами $(\eta'\sigma') \in (C(\sigma)\backslash\langle\sigma\rangle) \times (C(\eta)\backslash\langle\eta\rangle)$, що задовольняють початковим умовам $\alpha(a) = \varphi(a)$ і $\alpha(x) = \varphi(x)$. В підсумку отримуємо задачу $\Omega_2(Y, R)$, де Y - множина автоморфізмів R, отриманих за допомогою пар $(\sigma', \eta') \in [(C(\sigma)\backslash\langle\sigma\rangle) \times (C(\eta)\backslash\langle\eta\rangle)]$, що еквівалентно повному перебору секретних ключів.

Для оцінки складності взламу криптосхеми зловмисником, розглянемо потужність множини, елементи якої потрібно перебрати. Тоді складність даної атаки дорівнює $t_4 * t_6$. Тому при виборі параметрів безпеки, ця задача виявляється досить складною [1].

У випадку, якщо криптоаналітик має декілька криптограм, навіть при умові фіксованих автоморфізмів σ та η задача зламу все рівно зводиться до повного перебору секретних ключів, так як вони кожного разу будуть різні.

Атака на сеансові ключі. Задача полягає в тому, щоб знайти автоморфізми ψ та χ, а далі розв'язати відносно m рівняння $m * \left[\chi\big(\varphi(a)\big) * \psi\big(\varphi(x)\big)\right] = h$, де h відома з криптограми. Нехай автоморфізм ϕ побудований за допомогою автоморфізмів σ_1, η_1, а автоморфізм χ - за допомогою (σ_2, η_2). Для того щоб знайти $\chi(x), \psi(a)$ таких що $\chi(a)\psi(x) = h_1$, де h_1 відомий з криптограми і перевірити співвідношення $\sigma_1, \eta_1 \in (\langle\sigma\rangle, \langle\eta\rangle)$ і $(\sigma_2, \eta_2) \in (\langle\sigma\rangle, \langle\eta\rangle)$.Це буде не легше ніж перебрати пари $(\sigma_1, \eta_1) \in (\langle\sigma\rangle, \langle\eta\rangle)$ і $(\sigma_2, \eta_2) \in (\langle\sigma\rangle, \langle\eta\rangle)$ (а це повний перебір відповідних автоморфізмів) з наступною перевіркою умови $\chi(a)\psi(x) = h_1$. Відповідно, знайдена вище складність дорівнює $t_3^2 * t_5^2$. Навіть при правильному виборі параметрів безпеки, ця задача буде занадто складною [1].

Атака з вибраним вихідним текстом. Ця атака включає в себе криптоаналітика, який хоче отримати $\chi\big(\varphi(a)\big)\psi\big(\varphi(x)\big) \in R$ з розв'язком рівняння $m \times \chi\big(\varphi(a)\big)\psi\big(\varphi(x)\big) = h$ відносно m за допомогою нового сеансу зв'язку з учасником B у якості учасника A. Навіть якщо учасник B повторить такий самий текст m, він повинен побудувати нові сеансові автоморфізми $\chi' \neq$ і$\psi' \neq \chi$. Тому криптоаналітик отримає не $m \times \chi\big(\varphi(a)\big)\psi\big(\varphi(x)\big) = h$ а $m\chi'\chi\big(\varphi(a)\big)\psi\big(\varphi(x)\big) = h$. І навіть якщо він розв'яже рівняння відносно $m\chi'\chi\big(\varphi(a)\big)\psi\big(\varphi(x)\big) = h$, нової інформації відносно $m\chi'\chi\big(\varphi(a)\big)\psi\big(\varphi(x)\big) = h$ він не отримає.

Висновки

Криптоалгоритм іменується ідеально стійким, коли можливо прочитати зашифрований блок даних перебравши всі можливі ключі до тих пір, поки повідомлення не виявиться осмисленим. Таким чином, у загальному випадку стійкість блочного шифру залежить від довжини ключа і зростає експоненціально з її зростанням. В цій роботі проведено дослідження, яке показало стійкість розробленого криптопротоколу на основі квазігруп, дало оцінку його захищеності від реалізації атак націлених на криптограму, вихідні тексти та сеансові ключі, які є автоморфізмами блокового шифру, побудованого на квазігрупах. Досліджений криптопротокол може бути впроваджений для захисту важливих даних від втручання зловмисників.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 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.

2. Буняк В.М., Шелепало (Крайнічук) Г.В. Аналіз криптосхеми над квазігруповими кільцями // Матеріали L науково-технічної конференції ВНТУ. 2021 (тут).

3. Cryptographic Primitives with Quasigroup Transformations. / A. Mileva // The Faculty of Natural Science Library. – 2009. – 73-126 с.

Лавров Вадим Валерійович — студент групи 2БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vadosssss228@gmail.com

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

Lavrov Vadym V. — Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vadosssss228@gmail.com

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