КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.113121
УДК 621.391:519.2

Котух Євген Володимирович
кандидат технічних наук, доцент, професор кафедри кібербезпеки
Національний Технічний Університет «Дніпровська політехніка», Дніпро, Україна
ORCID 0000-0003-4997-620X
yevgenkotukh@gmail.com

Марухненко Олександр Сергійович
аспірант кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID 0000-0002-0583-3752
marukhnenko.oleksandr@gmail.com

Халімов Геннадій Зайдулович
доктор технічних наук, професор, завідувач кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID 0000-0002-2054-9186
hennadii.khalimov@nure.ua

Коробчинський Максим Володимирович
доктор технічних наук, професор, начальник 2-ї кафедри 2-го навчального факультету
Воєнна академія імені Євгенія Березняка Міністерства оборони України, м. Київ, Україна
ORCID 0000-0001-8049-4730
mars_kor@ukr.net

РОЗРОБКА МЕТОДИКИ ВИПРОБУВАНЬ БІБЛІОТЕКИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЮВАНЬ НА ПРИКЛАДІ КРИПТОСИСТЕМИ MST3 НА ОСНОВІ УЗАГАЛЬНЕНИХ СУЗУКІ 2-ГРУП

Анотація. У статті запропоновано методику випробувань бібліотеки криптографічних перетворень з реалізацією покращеної схеми шифрування на узагальнених Сузукі 2-групах криптосистемі MST3. Необхідність удосконалення наявних методів створення криптосистем викликана прогресом у розробці квантових комп'ютерів, які володіють достатньою обчислювальною міццю для вразливості багатьох існуючих криптосистем з відкритим ключем. Особливо це стосується систем, заснованих на факторизації та дискретному логарифмуванні, таких як RSA та ECC. За останні майже 20 років з'явилися пропозиції щодо використання некомутативних груп для розробки квантово-стійких криптосистем. Нерозв'язна проблема слова, сформульована Вагнером та Магьяриком, використовує групи перестановок і є перспективним напрямом у розробці криптосистем. Магліверас запропонував логарифмічні підписи, які є особливим типом факторизації, застосовуваною до скінченних груп, і останній варіант цієї технології відомий як MST3, заснований на групі Сузукі. Перша реалізація криптосистеми на узагальненій 2-групі Сузукі мала обмеження у шифруванні та захисті від атак повного перебору. За останні роки сформульовано багато пропозицій щодо покращення базової конструкції. Проведені авторами дослідження розширили можливості використання публічної криптографії з вдосконаленням параметрів на основі неабелевих груп. У статті продемонстрована методика проведення випробувань практичної реалізації бібліотеки криптографічних перетворень з реалізацією покращеної схеми шифрування на Сузукі 2-групах, підтверджено її працездатність.

Ключові слова: логарифмічний підпис; покриття; криптосистема MST3, узагальнені Сузукі-2 групи; схема шифрування.

ISSN 2663 - 4023

ВСТУП

У сучасному світі криптографічна безпека стає одним з ключових факторів захисту інформації та забезпечення конфіденційності даних. Останніми роками технологія квантових комп'ютерів, яка демонструє колосальний потенціал у розрахункових можливостях, поставила під загрозу багато сучасних криптосистем. Це зумовлено тим, що квантові алгоритми, такі як алгоритм Шора, можуть ефективно розбивати числа на множники, що робить небезпечним використання більшості сучасних асиметричних криптосистем.

Було запропоновано багато криптосистем з відкритим ключем, але лише деякі з таких систем залишаються непорушними. Більшість із них ґрунтується на сприйнятті нерозв'язності певних математичних проблем у дуже великих, скінченних циклічних групах у певних конкретних уявленнях. Найважливішими складними проблемами є:

1. проблема розкладання великих цілих чисел на множники;
2. проблема представлення великих циклічних груп;
3. пошук короткого базису для заданої великої інтегральної решітки L.

На жаль, з огляду на квантові алгоритми Шора для цілочисельної факторизації та вирішення проблеми дискретного логарифма [1] відомі системи з відкритим ключем стануть небезпечними з розповсюдженням квантових комп'ютерів. Доповідь під редакцією П. Нгуєна [2] визначає ці та інші проблеми, які стоять перед сферою інформаційної безпеки в майбутньому.

Постановка проблеми. Логарифмічні підписи для кінцевих груп є невід'ємною складовою криптосистем з відкритим ключем MST1 та MST3. Важливим питанням щодо використання MST3 стало створення нових класів логарифмічних підписів із властивостями, яких не мають трансверсальні (у тому числі злиті) логарифмічні підписи. Для цього Баумейстер та де Вільєс представили новий метод побудови аперіодичних логарифмічних підписів для абелевих груп. Наприкінці 1970-х років Спіросом Магліверасом розпочато дослідження придатності особливої факторизації для кінцевих неабелевих груп — логарифмічного підпису, для використання у криптографії [3], [4]. Пізніше було опубліковано роботи Магліверасом, Траном ван Трунгом та Стінсоном, де описуються розроблені Магліверасом криптографічні системи — MST1 на основі логарифмічних підписів та MST2 на основі альтернативного типу покриттів — так званих [s, r]-осередках. Перешкодою є відсутність будь-якої відомої практичної реалізації MST1 або MST2. Пізніше ним було розроблено іншу криптосистему на основі відкритих ключів — MST3, що поєднує попередні та використовує логарифмічні підписи та випадкові покриття кінцевих неабелевих груп. 2-групи Сузукі пропонуються як потенційний базовий елемент для реалізації цієї криптосистеми.

Отже, криптосистеми з відкритим ключем MST1 [3] та MST3 [5], [6] було розроблено на основі логарифмічних підписів — своєрідної факторизації кінцевих груп. Основна ідея побудови MST3 полягає у побудові однобічних функцій з потайним входом (люком), використовуючи випадкові покриття для кінцевих неабелевих груп з великим центром. [6], [7] Інтегрована інформація про люк, що є основною частиною закритого ключа схеми, використовує логарифмічні підписи центру.

У нещодавньому документі [10] Баумейстер та де Вільєс пропонують цікавий алгоритм для створення аперіодичних логарифмічних підписів для абелевих груп, зокрема, для абелевих 2-груп, які перешкоджають атаці Блекбьорна та інших. Варто зазначити, що трансверсальні (у тому числі злиті) логарифмічні підписи є періодичними. У роботі [10] буде введено поняття повністю аперіодичних логарифмічних підписів та представлено їхню побудову для абелевих p-груп на основі алгоритму Баумейстера-де

Вільєса. Аперіодичні і повністю аперіодичні логарифмічні підписи забезпечують такі класи логарифмічних підписів, що відповідають використанню MST3. Модифікована у такий шлях MST3 є об'єктом дослідження роботи. Більше того, повністю аперіодичні логарифмічні підписи для абелевих груп самі по собі представляють теоретичний інтерес.

Аналіз останніх досліджень і публікацій. Проблемами використання некомутативних груп в побудові схем шифрування в різні роки займались Н. Вагнер, М. Маг'ярик, С. Магліверас, В. Шпильрейн, Д. Кахробай. Вдосконаленням ідей побудови квантово стійкої криптографії з використанням криптосистеми MST3 займались А. Нусс, П. Сваба, Т. Ван Трунг, В. Лемпкен, В. Вей, Й. Конг, Х. Хонг, Ж. Шао, С. Хан, Ж. Лин, С. Жао. 2-групи Сузукі було запропоновано як основні групи для створення MST3 — їхня проста структура дозволяє більш уважне дослідження безпечності системи та більш ефективну її реалізацію. Перший аналіз спрощеної версії MST3 [5], здійснений Магліверасом, Свабою, ван Трунгом та Заяцем [8], показує, що трансверсальні логарифмічні підписи непридатні для використання у схемі. Подальші дослідження Блекбьорна, Сіда та М'юллана [9] доводить, що використання злитих трансверсальних логарифмічних підписів також робить спрощену версію MST3 небезпечною. Однак для посиленої версії MST3 [6] вони все ще витримують потужну атаку перестановкою матриць [6]. Тому є доцільним вивчити додаткові класи логарифмічних підписів з особливостями, що роблять їх більш придатними для використання у криптосистемах з відкритим ключем на кшталт MST3.

Автори статті оприлюднили результати дослідницької роботи, що демонструє подальше вдосконалення MST3 [11] – [19]. Нажаль, практичній реалізації приділяється дуже мало уваги, що створює передумови для дослідницької роботи, що мала б на меті висвітлення методики практичних випробувань схем шифрування в режимах генерації ключової пари, шифрування, дешифрування тощо.

Мета статті. Стаття присвячена розробці методики випробувань криптосистеми MST3 на основі узагальнених Сузукі 2-груп. Ця криптосистема є однією з можливих відповідей на виклики, які ставить перед нами технологія квантових обчислень. Особливо актуальним є впровадження таких систем на державному рівні в Україні, адже захист інформації є стратегічно важливим для національної безпеки країни та її інформаційних ресурсів.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Схема побудови криптосистема MST детально розглянута в [X]. Розглянемо G як кінцеву неабелеву групу. Група має нетривіальний центр $\mathbf{z}$, тому G не розкладається над $\mathbf{z}$. Припустимо, що $\mathbf{z}$ настільки великий, що пошук $\mathbf{z}$ є обчислювально непрактичним. Якщо $\alpha=[A_1,...,A_s]$ є логарифмічним підписом, а кожен елемент $g\in G$ може бути однозначно виражений як добуток виду $g=a_1\cdot a_2\cdots a_s$, для $a_i\in A_i$. $\alpha=[A_1,...,A_s]$ то такий підпис називається простим (таким, що розкладається на множники), якщо його можна розкласти на багаточлен w шириною G.

Криптографічна гіпотеза, яка є основою для криптосистеми, полягає в тому, що якщо $\alpha=[A_1,A_2,...,A_s]:=(a_{i,j})$ — випадкова накладка на «великий» матрац S на G, то шукати образ $g=a_{1j_1}a_{2j_2}\cdots a_{sj_s}$ є обчислювально непрактичним для будь-якого елемента $g\in G$ відносно α. Теоретичні основи побудови схем асиметричного шифрування, а також експериментальні результати розрахунків показано в.

ПРАКТИЧНІ ВИПРОБУВАННЯ БІБЛІОТЕКИ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Метою випробувань системи є перевірка працездатності бібліотеки ра її роботи в усіх режимах випробувань (див. табл. 2) для прийняття системи в тестову експлуатацію з формуванням акту випробувань.

Для отримання результатів криптографічних перетворень бібліотека працює в трьох заданих режимах: генерація ключової пари, шифрування та дешифрування. Результати випробувань будуть представлені для всіх режимів роботи бібліотеки з урахуванням наступних параметрів:

- Вибір групи та кількості координат (за замовченням група Сузукі з кількістю координат, що дорівнюють 5 точкам);
- Довжина функціонального поля (128, 256 чи 512);
- Довжина блока логарифмічних підписів (32, 64 чи 128).

З метою уніфікації результатів роботи кожного з режимів генерації ключів, шифрування та дешифрування домовимся використовувати наступний підхід:

В якості маски назви для згенерованих ключів використовуємо:

SerXXXX-SAA-FBB-LCC-KEY.ASC, де:

- SerXXXX — унікальний серійний номер ключової пари (генерується починаючи з 00001 та перевіряється чи є наявні ключи в теці розташування, якщо ключі з 00001 існує, то далі ім’я присвоюється інкрементально);
- SAA — S — визначена група (S — група Сузукі), AA — кількість координат в групі. Для завдань тестування та з урахуванням потужності комп’ютерів, що використовуються зафіксуємо кількість координат еквівалентно 5;
- FBB — F — функціональне поле довжиною BB, де BB — довжина функціонального поля, що дорівнює відповідно 128, 256 чи 512 біт;
- BCC — B — логарифмічний підпис з довжиною блока CC, де CC — довжина блока, що дорівнює відповідно 32, 64 чи 128 біт;
- KEY — тип ключа в ключовій парі, де KEY=PUB — публічний ключ, KEY=SEC — секретний ключ з відповідної ключової пари з унікальний серійним номером;
- *.ASC — розширення файлів ключової пари.

Бібліотека викликається за допомогою командної строки в наступному форматі:

MST3_GS.exe команда параметри

Всі режими випробувань та варіанти використання параметрів виклику команд представлені в Таблиці 2.

Таблиця 2

Представлення логарифмічного підпису

Режим	Виклик команди	Очікувані результати
Генерація ключів	MST3-GS.exe keygen -s5 -f128 -b32	Згенерована ключова пара (публічний та секретний ключі) згідно з параметрами, що були використані у виклику команди в командній строчці
	MST3-GS.exe keygen -s5 -f128 -b64	
	MST3-GS.exe keygen -s5 -f128 -b128	
	MST3-GS.exe keygen -s5 -f256 -b32	
	MST3-GS.exe keygen -s5 -f256 -b64	
	MST3-GS.exe keygen -s5 -f256 -b128	
	MST3-GS.exe keygen -s5 -f512 -b32	
	MST3-GS.exe keygen -s5 -f512 -b64	
	MST3-GS.exe keygen -s5 -f512 -b128	

Шифрування	MST3-GS.exe encrypt SerXXXXX-s5f128b32-pub.asc text.txt MST3-GS.exe encrypt SerXXXXX-s5f128b64-pub.asc text.txt MST3-GS.exe encrypt SerXXXXX-s5f128b128-pub.asc text.txt MST3-GS.exe encrypt SerXXXXX-s5f256b32-pub.asc text.txt MST3-GS.exe encrypt SerXXXXX-s5f256b64-pub.asc text.txt MST3-GS.exe encrypt SerXXXXX-s5f256b128-pub.asc text.txt MST3-GS.exe encrypt SerXXXXX-s5f512b32-pub.asc text.txt MST3-GS.exe encrypt SerXXXXX-s5f512b64-pub.asc text.txt MST3-GS.exe encrypt SerXXXXX-s5f512b128-pub.asc text.txt	Здійснено шифрування тексту text.txt з використанням згенерованого публічного ключа відповідно до кожного сценарію та створено відповідне зашифроване повідомлення
Дешифрування	MST3-GS.exe decrypt SerXXXXX-s5f128b32-sec.asc encrypted.txt MST3-GS.exe decrypt SerXXXXX-s5f128b64-sec.asc encrypted.txt MST3-GS.exe decrypt SerXXXXX-s5f128b128-sec.asc encrypted.txt MST3-GS.exe decrypt SerXXXXX-s5f256b32-sec.asc encrypted.txt MST3-GS.exe decrypt SerXXXXX-s5f256b64-sec.asc encrypted.txt MST3-GS.exe decrypt SerXXXXX-s5f256b128-sec.asc encrypted.txt MST3-GS.exe decrypt SerXXXXX-s5f512b32-sec.asc encrypted.txt MST3-GS.exe decrypt SerXXXXX-s5f512b64-sec.asc encrypted.txt MST3-GS.exe decrypt SerXXXXX-s5f512b128-sec.asc encrypted.txt	Здійснено дешифрування зашифрованого повідомлення з використанням згенерованого секретного ключа відповідно до кожного сценарію та коректно відновлено оригінальне відкрите текстове повідомлення

У рамках цієї роботи проведемо випробування бібліотеки криптографічних перетворень з параметрами s5, f128 та b32. Послідовність виклику команд та очікувані результати представлено в Табл. 3–5.

Таблиця 3

Режим генерація ключової пари

№	Назва	Кроки	Очікуваний результат
	передумова	Завантажена операційна система Windows, відкрита командний рядок	
1	Ініціація серії сценаріїв 1–3	Створити теку C:\Test та скопіювати файли MST3-GS.exe та MST3_GeneralSuzuki.dll в теку. Створити файл test.txt з будь-яким повідомленням, що буде використовуватися в якості відкритого тексту.	На диску C створена тека Test. В теці знаходяться файли MST3-GS.exe, MST3_GeneralSuzuki.dll та текстовий файл test.txt.
1	Виклик бібліотеки з командою генерації ключової пари та параметрами згідно Сценарію 1	MST3-GS.exe keygen -s5 -f128 -b32	В теці місцезнаходження бібліотеки були згенеровані ключі з наступними назвами файлів: ser00001-s5b32f128-pub.asc ser00001-s5b32f128-sec.asc

Таблиця 4

Режим шифрування

№	Назва	Кроки	Очікуваний результат
	передумова	Завантажена операційна система Windows, відкрита командний рядок, користувач перейшов в командній строчці до шляху виконуваного файлу бібліотеки, виконано Сценарій 1. В теці бібліотеки знаходяться файли MST3-GS.exe та MST3_GeneralSuzuki.dll, текстовий файл test.txt з відкритим текстом повідомлення та ключова пара файли ser00001-s5b32f128-pub.asc та ser00001-s5b32f128-sec.asc.	
1	Виклик бібліотеки з командою шифрування та параметрами згідно Сценарію 2	MST3-GS.exe encrypt ser00001-s5b32f128-pub.asc test.txt	В теці місцезнаходження бібліотеки був згенерований файл, що є зашифрованим текстом відкритого повідомлення test.txt та має назву testser00001encrypted.txt

Таблиця 5

Режим дешифрування

№	Назва	Кроки	Очікуваний результат
	Передумова	Завантажена операційна система Windows, відкрита командний рядок, користувач перейшов в командній строчці до шляху виконуваного файлу бібліотеки, послідовно виконано Сценарії 1 та 2. В теці бібліотеки знаходяться файли MST3-GS.exe та MST3_GeneralSuzuki.dll, текстовий файл test.txt з відкритим текстом повідомлення, ключова пара файли ser00001-s5b32f128-pub.asc та ser00001-s5b32f128-sec.asc, а також файл testser00001encrypted.txt з зашифрованим повідомленням.	
1	Виклик бібліотеки з командою шифрування та параметрами згідно Сценарію 3	MST3-GS.exe decrypt ser00001-s5b32f128-sec.asc testser00001encrypted.txt	В теці місцезнаходження бібліотеки був згенерований файл, що є дешифрованим текстом та має назву testdecrypted.txt Зміст файлу testdecrypted.txt повністю відповідає файлу test.txt
2	Завершення серії сценаріїв 1–3	Зайти в теку C:\Test. Видалити файли ключів ser00001-s5b32f128-pub.asc та ser00001-s5b32f128-sec.asc, зашифрований файл testser00001encrypted.txt та дешифрований файл testdecrypted.txt.	В теці знаходяться лише файли MST3-GS.exe, MST3_GeneralSuzuki.dll та текстовий файл test.txt.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Результати випробувань демонструють працездатність рішення для узагальненої групи Сузукі для п’яти координат з розміром блоку 32 біт та полем розмірністю 2^{128}. Бібліотека реалізує всі режими роботи та генерує криптографічні артефакти в режимах від 5 до 10 координат (такі параметри дозволяють ефективно використовувати архітектуру x86/ч64 та швидко робити обчислення), з розмірами блоків 32,64,128 біт та розмірністю поля $2^{128\text{-}512}$ біт. В подальшому має науковий та практичний інтерес реалізація бібліотеки криптографічних перетворень з іншими некомутативними групами, а також впровадження методики та практичних результатів випробувань в освітній процес ЗВО України з розробкою лабораторних робіт та візуалізацію переваг та недоліків рішення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shor, P. (1999). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM, 41(2),* 303–332.
2. Nguyen, P. (2009). Recent Trends in Cryptography. *Contemporary Mathematics, 477,* 883–887.
3. Magliveras, S. Oberg, B., & Surkan, A. (1984). A new random number generator from permutation groups. *Physico-mathematical Milan symposium,* 203–223.
4. Magliveras, S., & Memon, N. (1992). Algebraic properties of cryptosystem PGM. *Journal of Cryptology,* 167–183.
5. Staszewski, R., & Trung, T. (2018). Strongly aperiodic logarithmic signatures, *Essen: Duisburg-Essen.*
6. Blackburn, S., Cid, C., & Mullan, C. (2009). Cryptanalysis of the MST3 public key cryptosystem. *Journal of Mathematics and Cryptology*, 321–338.
7. Magliveras, S., Trung, T., & Stinson, D. (2002). New Approaches to Designing Public Key Cryptosystems Using One-Way Functions and Trapdoors in Finite Groups. *Journal of Cryptology*, 285–297.
8. Svaba, P., & Trung, T. (2010). MST3 public key cryptosystem: cryptanalysis and implementation. *Journal of Mathematics and Cryptology*, 271–315.
9. Magliveras, et al. (2008). On the security of a realization of cryptosystem MST3. *Mathematical publications Tatra Mountains*, 1–13.
10. Баумейстер, Б., & Вільєс де Д. (2012). Аперіодичні логарифмічні підписи. *J. Math. Cryptol. 6,* 21–37.
11. Kotukh, Y., et al. (2021). Some results of development of cryptographic transformations schemes using non-abelian groups. *Radio engineering, 204*, 66–72.
12. Котух, Є., Сєвєрінов, О., Власов, В. та ін. (2021). Методи побудови та властивості логарифмічних підписів. *Радіотехніка, 205*, 94–99. https://doi.org/10.30837/rt.2021.2.205.09
13. Kotukh, Y., Khalimov, G. (2021). Hard Problems for Non-abelian Group Cryptography. *Fifth International Scientific and Technical Conference "Computer and Information systems and technologies".* https://doi.org/10.30837/csitic52021232176
14. Халімов, Г., Котух, Є., Сергійчук, Ю., & Марухненко, О. (2018). Аналіз складності реалізацій криптосистеми на групі Сузукі. *Радіотехніка, 193*, 75–81.
15. Котух, Є., Охріменко, Т., Дяченко, О., Ротаньова, Н., Козіна, Л., & Зеленський, Д. Криптоаналіз систем на основі проблеми слова з використанням логарифмічних підписів. *Радіотехніка, 206*, 106–114. https://doi.org/10.30837/rt.2021.3.206.09
16. Kotukh, Y., Khalimov, G. (2022). Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures. In *Proceedings of II International Conference Information security: problems and prospects*, 55–58
17. Magliveras, S., Stinson, D., & Trung van, T. (2002). New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups. *Journal of Cryptology, 15*, 285–297.
18. Khalimov, G., et al. (2021). Towards advance encryption based on a Generalized Suzuki 2-groups. *International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME),* 1–6. https://doi.org/10.1109/ICECCME52200.2021.9590932
19. Khalimov, G., Kotukh, Y., & Khalimova, S. (2020). MST_3 Cryptosystem Based on a Generalized Suzuki 2-Groups. *Copyright, 2711*. http://ceur-ws.org/Vol-2711/paper1.pdf

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Yevgen Kotukh
PhD, associate professor, professor of the cyber security department
National Technical University "Dniprovsk Polytechnic"; Dnipro, Ukraine
ORCID 0000-0003-4997-620X
yevgenkotukh@gmail.com

Oleksandr Marukhnenko
Graduate student of the Department of Information Technology Security
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID 0000-0002-0583-3752
marukhnenko.oleksandr@gmail.com

Hennadii Khalimov
Doctor of Science, professor, head of the Information Technology Security Department
Kharkiv National University of Radio Electronics; Kharkiv, Ukraine
ORCID 0000-0002-2054-9186
hennadii.khalimov@nure.ua

Maksym Korobchynskyi
Doctor of Science, professor, head of the 2nd department of the 2nd educational Faculty
Yevgeny Bereznyak Military Academy of the Ministry of Defense of Ukraine, Kyiv, Ukraine
ORCID 0000-0001-8049-4730
mars_kor@ukr.net

DEVELOPMENT OF METHODS FOR TESTING THE LIBRARY OF CRYPTOGRAPHIC TRANSFORMATIONS ON THE EXAMPLE OF THE MST3 CRYPTOSYSTEM BASED ON GENERALIZED SUZUKI 2-GROUPS

Abstract. The article proposes a methodology for testing a library of cryptographic transformations with the implementation of an improved encryption scheme on generalized Suzuki 2-groups in the MST3 cryptosystem. The need to improve existing methods of cryptosystem creation is driven by progress in quantum computer development, which possess sufficient computational power to compromise many existing public key cryptosystems. This is especially true for systems based on factorization and discrete logarithm, such as RSA and ECC. Over the last nearly 20 years, there have been proposals for using non-commutative groups to develop quantum-resistant cryptosystems. The unsolved word problem, formulated by Wagner and Magyarik, uses permutation groups and is a promising direction in cryptosystem development. Magliveras proposed logarithmic signatures, a special type of factorization applied to finite groups, and the latest version of this technology is known as MST3, based on the Suzuki group. The first implementation of the cryptosystem on the generalized Suzuki 2-group had limitations in encryption and protection against brute force attacks. Over the past years, many proposals have been made to improve the basic design. The research conducted by the authors expanded the possibilities of using public cryptography by refining parameters based on non-Abelian groups. The article demonstrates the methodology for conducting tests of the practical implementation of the library of cryptographic transformations with the implementation of an improved encryption scheme on Suzuki 2-groups, confirming its functionality.

Keywords: logarithmic signature; covers; MST3 cryptosystem; generalized Suzuki-2 groups; encryption scheme.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Shor, P. (1999). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM, 41(2),* 303–332.
2. Nguyen, P. (2009). Recent Trends in Cryptography. *Contemporary Mathematics, 477,* 883–887.
3. Magliveras, S. Oberg, B., & Surkan, A. (1984). A new random number generator from permutation groups. *Physico-mathematical Milan symposium,* 203–223.
4. Magliveras, S., & Memon, N. (1992). Algebraic properties of cryptosystem PGM. *Journal of Cryptology,* 167–183.

5. Staszewski, R., & Trung, T. (2018). Strongly aperiodic logarithmic signatures, *Essen: Duisburg-Essen.*
6. Blackburn, S., Cid, C., & Mullan, C. (2009). Cryptanalysis of the MST3 public key cryptosystem. *Journal of Mathematics and Cryptology*, 321–338.
7. Magliveras, S., Trung, T., & Stinson, D. (2002). New Approaches to Designing Public Key Cryptosystems Using One-Way Functions and Trapdoors in Finite Groups. *Journal of Cryptology*, 285–297.
8. Svaba, P., & Trung, T. (2010). MST3 public key cryptosystem: cryptanalysis and implementation. *Journal of Mathematics and Cryptology*, 271–315.
9. Magliveras, et al. (2008). On the security of a realization of cryptosystem MST3. *Mathematical publications Tatra Mountains*, 1–13.
10. Baumeister, B., & Villiers de D. (2012). Aperiodic logarithmic signatures. *J. Math. Cryptol. 6*, 21–37.
11. Kotukh, Y., et al. (2021). Some results of development of cryptographic transformations schemes using non-abelian groups. *Radio engineering, 204*, 66–72.
12. Kotukh, Y., et al. (2021). Construction methods and properties of logarithmic signatures. *Radio engineering, 205*, 94–99. https://doi.org/10.30837/rt.2021.2.205.09
13. Kotukh, Y., Khalimov, G. (2021). Hard Problems for Non-abelian Group Cryptography. *Fifth International Scientific and Technical Conference "Computer and Information systems and technologies".* https://doi.org/10.30837/csitic52021232176
14. Halimov, G., et al. (2018). Analysis of the complexity of cryptosystem implementations on the Suzuki group. *Radio engineering, 193*, 75–81.
15. Kotukh, Y., et al. Cryptoanalysis of systems based on the word problem using logarithmic signatures. *Radio engineering, 206*, 106–114. https://doi.org/10.30837/rt.2021.3.206.09
16. Kotukh, Y., Khalimov, G. (2022). Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures. In *Proceedings of II International Conference Information security: problems and prospects*, 55–58
17. Magliveras, S., Stinson, D., & Trung van, T. (2002). New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups. *Journal of Cryptology, 15*, 285–297.
18. Khalimov, G., et al. (2021). Towards advance encryption based on a Generalized Suzuki 2-groups. *International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 1–6. https://doi.org/10.1109/ICECCME52200.2021.9590932
19. Khalimov, G., Kotukh, Y., & Khalimova, S. (2020). MST_3 Cryptosystem Based on a Generalized Suzuki 2-Groups. *Copyright, 2711*. http://ceur-ws.org/Vol-2711/paper1.pdf