менеджера / В. М. Заяць // Актуальні проблеми економіки. – 2009. – № 6 (96). – С. 280–288. 7. Гарнаев А. Ю. Самоучитель VBA / А. Ю. Гарнаев. – 2-е изд., перераб и доп. – СПб.: БХВ-Петербург, 2004. – 560 с. 8. Сороківська О. А., Гевко В. Л. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету. – 2010. – № 2, Т. 2. – С. 32–35. 9. Галатенко В.А. Основы информационной безопасности / В.А. Галатенко. – М.: Изд-во "Интернет-университет информационных технологий – ИНТУИТ.ру", 2003. – 280 с.

УДК 003.26.09:004.032.24

О. Кравець, С. Лупенко, А. Луцків
Тернопільський національний технічний університет ім. І. Пулюя,
кафедра комп'ютерних систем та мереж,

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КРИПТОАНАЛІЗУ СУЧАСНИХ ПОТОКОВИХ ШИФРІВ

Розглянуто підвищення ефективності криптоаналізу сучасних потокових шифрів. Проаналізовано сучасне програмне забезпечення для здійснення алгебраїчного криптоаналізу потокових шифрів. Запропоновано шляхи оптимізації сучасних криптоаналітичних методів потокових шифрів шляхом використання паралельних та розподілених високопродуктивних обчислювальних засобів.

Ключові слова: криптоаналіз, потокові шифри, високопродуктивні обчислення, обчислювальні кластери.

Increasing efficiency of cryptanalysis of the modern stream ciphers this paper is devoted. Modern software for the algebraic cryptanalysis of stream ciphers are analyzed in article. The ways of optimization of modern cryptanalysis methods for stream ciphers by using parallel and distributed high-performance and data processing systems are proposed.

Key words: cryptanalysis, stream ciphers, high-performance computing, computational clusters.

Вступ. Загальна постановка проблеми

Криптостійкість потокових алгоритмів шифрування, тобто стійкість до криптографічної атаки за певних фіксованих умов вимірюється потрібною кількістю ресурсів для проведення криптоатаки. Ресурсами є такі величини:

1. Кількість інформації, яка необхідна для здійснення успішної атаки, а саме – необхідна кількість пар відомих або вибраних текстів.

2. Обчислювальна складність алгоритму криптоаналізу визначається ресурсами, необхідними для його виконання, і є функцією, яка визначає залежність обсягу роботи, що виконується цим алгоритмом від розміру вхідних даних. На практиці виділяють дві складові обчислювальної складності: T (часову складність) і S (просторову складність або вимоги до пам'яті). T і S, як правило, подаються як функції від n, де n – розмір вхідних даних, тобто кількість відкритих і/або зашифрованих даних.

Так, величина T – час, який необхідний для здійснення успішної атаки, визначається кількістю тестових операцій шифрування атакуючим алгоритмом, виконання яких за дотримання інших необхідних умов дає змогу, наприклад, визначити ключ шифрування.

Величина S – вказує на обсяг пам'яті, який необхідний для проведення успішної атаки. Ціла низка криптоатак не може бути реалізована на практиці у зв'язку з недостатнім обсягом оперативної та дискової пам'яті. Цей параметр визначає просторову складність криптоалгоритму.

Розглянемо детальніше ці складові.

1. Під час перехоплення трафіку переважно реалізується атака "man-in-the-middle", – тобто активне або пасивне перехоплення трафіку. Це завдання істотно спрощується, якщо

використовуються безпровідні мережі зв'язку, – у такому випадку можливим є використання типових користувацьких пристроїв. Для роботи з проводовими каналами зв'язку також є багато спеціалізованих пристроїв [1]. У сучасних цифрових мережах передачі даних значна частина інформації є службовою, тому можна порівняно просто передбачити вміст пакетів, що передаються. А кількість пар відкритих текстів та відповідних їм зашифрованих визначається інтенсивністю трафіку та часом перехоплення інформації.

2. Часова характеристика T обчислювальної складності визначає кількість часу, необхідного для здійснення криптоаналізу потокового шифру.

У технічних характеристиках потокових шифрів зазначають теоретичну криптостійкість, яка визначає стійкість шифру до методу повного перебору і, як правило, є 2^m, де m – довжина ключа.

Стійкість до інших методів криптоаналізу, а саме – диференціального, лінійного та інших, є якісною характеристикою. Теоретична криптостійкість більшості потокових шифрів ґрунтується на проблемах обчислюваної складності, які належать до *NP*-класу складності. Задача криптоаналітика полягає у відшуканні такого алгоритму криптоаналізу, який міг би бути розв'язаний за поліноміальний час, тобто шуканий криптоаналітичний алгоритм мав би належати до *P*-класу обчислювальної складності. Просторова характеристика S може бути оцінена шляхом обрахунку типів даних та їх розмірності на усіх етапах криптоаналітичного дослідження.

У цьому аспекті доцільно згадати про т. зв. "time-memory tradeoff"-методи, які передбачають за умови недостатніх процесорних ресурсів часу задіювати ресурси пам'яті, зокрема використання "райдужних" таблиць. Успішним прикладом використання райдужних таблиць є криптоаналіз алгоритму A5 [2].

Зв'язок висвітленої проблеми із важливими науковими та практичними завданнями

Збільшення кількості мереж передачі даних різного призначення та масштабу з різноманітними фізичними середовищами передачі даних (проводових та безпроводових), робота яких ґрунтується на різноманітних протоколах і які мають різні архітектури, передбачає розробку надійних систем їх захисту. Системи захисту реалізовані у відповідних протоколах та алгоритмах шифрування. Досить часто у мережах передачі даних, зокрема безпроводових, використовуються потокові алгоритми шифрування, що зумовлено низькими обчислювальними потужностями, необхідними для функціонування алгоритму шифрування та особливостями протоколів передачі даних. До найвідоміших технологій належать: стандарт GSM (алгоритми A5/1, A5/2), UMTS (алгоритм UEA2/UIA2 (інші назви A5/4, SNOW 3G)), стандарт CDMA2000 (алгоритм ORYX), стандарт IEEE 802.11 b/g (алгоритм RC4 (протокол WEP)), стандарт IEEE 802.15.1-2002 (алгоритм E0), стандарт Geostationary Earth Orbit (GEO) Mobile Radio Interface (алгоритми GMR-1, GMR-2) тощо.

Криптостійкість деяких із наведених алгоритмів є незадовільною. Це зумовлено створенням нових методів та засобів криптоаналізу, тому необхідно здійснити верифікацію існуючих та створюваних алгоритмів шифрування.

Актуальність теми зумовлена необхідністю створення нових криптостійких до різних типів атак потокових шифрів та верифікації вже існуючих. Важливим є чинник появи нового криптоаналітичного апарата, до якого можна зарахувати алгебраїчний криптоаналіз [3], а також зменшення ціни на високопродуктивні обчислювальні засоби, що робить їх доступнішими для потенційних зловмисників.

Мета і завдання дослідження

Мета роботи – проаналізувати наявне математичне та програмне забезпечення криптоаналізу сучасних потокових шифрів для виявлення чинників, які дадуть змогу підвищити його ефективність. Розглянемо основні кроки, необхідні для досягнення поставленої мети:

1. Аналіз сучасних криптоаналітичних методів та найчастіше використовуваних алгоритмів шифрування.
2. Аналіз наявного криптоаналітичного програмного забезпечення та формулювання вимог до розроблення власного (модифікації існуючого).

3. Виявлення основних чинників, які дадуть змогу підвищити його ефективність, зокрема шляхом використання високопродуктивних обчислювальних засобів.

Аналіз останніх досліджень та публікацій

Розглянемо методи криптоаналізу сучасних потокових шифрів (таблиця). Варто зазначити, що більшість методів криптоаналізу дають змогу отримати результат лише з певною ймовірністю, водночас повторення криптоаналітичного експерименту з іншими вхідними параметрами дає змогу підвищити ймовірність.

Характеристики поширених потокових алгоритмів шифрування

Потоковий шифр	Дата створення	Розробник (патент/ стандарт)	Атака		Крипто-стійкий на даний час	Застосування
			найбільш відома	обчислювальна складність		
A5/1, A5/2	1987, 1989	Частина GSM-стандарту	На основі відомих відкритих текстів (райдужні таблиці, “time-memory tradeoff”)	2^{39}	ні	шифрування голосу у GSM-мережах
GEA5/1, GEA5/2	1993	Частина GSM-стандарту	Атака “розділяй і володарюй” (“time-memory tradeoff”)	2^{45}	ні	шифрування даних у GSM-мережах
Achterbahn-128/80	2006	Берндт Ґамел, Рейнер Ґотферт, Олівер Найфер	Підбір для довжини фрейму $L \leq 244$. Кореляційна атака для $L \geq 248$.	2^{80}	так	Проект eSTREAM (EU ECRYPT)
FISH	1993	Siemens	Текстова атака	2^{11}	ні	Телефонія
E0	1999	Частина стандарту IEEE 802.15.1	Статична атака	2^{64}	так	Bluetooth
RC4	1987	Рон Райвест	На основі відомих відкритих текстів	2^{13} (2^{33})	ні	Протоколи SSL, WEP
Salsa20	До -2004	Деніел Бернстейн	Метод ймовірнісно-нейтральних бітів	2^{251} для 8 раундів	так	Проект eSTREAM (EU ECRYPT)
Scream	2002	Шай Холеві, Дон Коперсміт та Чаранжит Жутала	-	-	так	Шифрування даних на жорстких магнітних дисках
SEAL	1997	U.S. Patent 5,454,039, U.S. Patent 5,675,652	Метод ймовірнісно-нейтральних бітів	-	ні	Шифрування даних на жорстких магнітних дисках
SNOW 3G 2.0	До-2003	ISO/IEC IS 18033-4	-	-	так	3rd Generation Partnership Project
SOSEMANUK	До-2004	Олівер Біллет, Ніколас Куртуа та ін. (без патентних обмежень)	-	-	так	3G-мережі
Turing	2000–2003	Ґрегорі Роуз і Філіп Хоукс (Qualcomm)	-	-	Так	CDMA-мережі

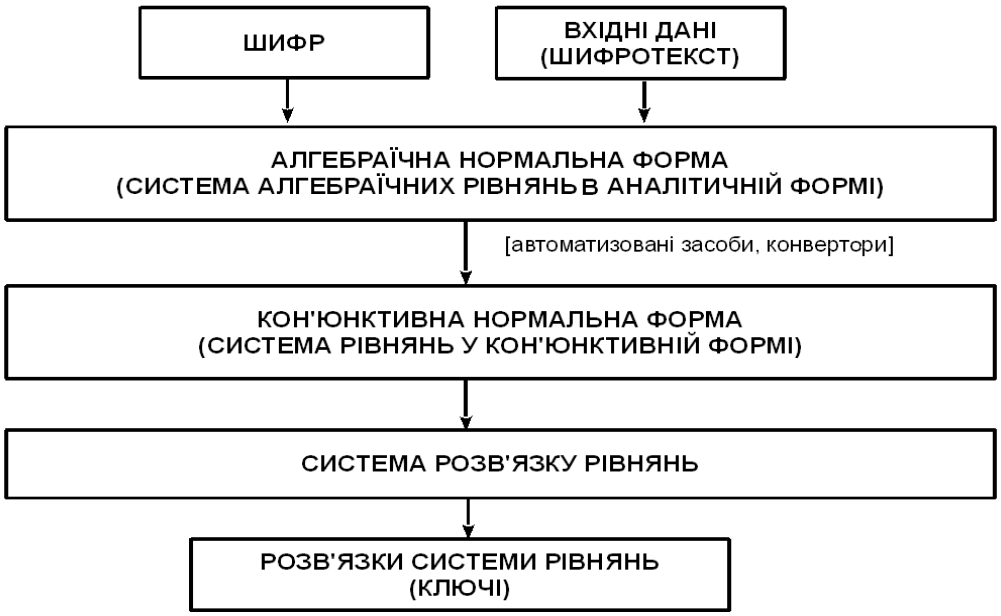
На основі теоретичних оцінок T та S, а також ймовірнісних характеристик отриманого результату, які вказують на кількість необхідних експериментів, можна отримати аналітичні значення часу та пам'яті для знаходження шуканих результатів. Врахування конкретних особливостей апаратно-програмних комплексів дає змогу отримати числові характеристики часу та пам'яті, які є близькими до абсолютних.

Найчастіше в ході криптоаналітичних досліджень використовуються диференціальний та лінійний методи [4], а також "mod n"-атака та метод пов'язаних ключів. До порівняно нових належить метод алгебраїчного криптоаналізу, який був уперше запропонований Н. Куртуа [3]. На думку авторів, цей метод є одним із найперспективніших, хоча його практичне використання й передбачає подальші дослідження. До його ключових особливостей порівняно з іншими варто зарахувати: універсальність (підходить як для потокових, так і для блокових шифрів), здатність масштабуватися, можливості подальшого вдосконалення.

Алгебраїчні криптоаналітичні методи – це методи, які передбачають подання криптографічних перетворень ключа, вхідних та вихідних даних для шифрування у вигляді деякого рівняння [3, 5]. Тоді сукупності таких перетворень формують систему рівнянь. Сьогодні є реалізації цього підходу для криптосистем, які мають практичне використання [6]. Проте його застосування для широкого кола шифросистем у багатьох випадках має теоретичний характер, або не є повною мірою досліджене сьогодні. Загальну схему алгебраїчного криптоаналізу показано на рисунку.

Можливість використання цього методу пов'язана з необхідністю розв'язання багатох теоретичних та прикладних задач, зокрема:

1. Представлення алгоритму шифрування у вигляді системи рівнянь в аналітичній формі.
2. Перетворення аналітичної форми криптоалгоритму до кон'юнктивної нормальної форми.
3. Розв'язання системи рівнянь у кон'юнктивній нормальній формі.
4. Якщо п.1 і п.2 вимагають чіткої математичної формалізації криптоаналітичної системи, то п.3 пов'язаний з числовим розв'язком відповідної системи рівнянь великої обчислювальної складності.



Загальна схема алгебраїчного криптоаналізу

У [7] було представлено AES-128 великою системою рівнянь: 8000 рівнянь з 1600 невідомими. У працях Н. Куртуа показано, що складність розв'язання системи квадратних рівнянь з багатьма невідомими може бути істотно спрощена, якщо система є розрідженою і має регулярну структуру, на прикладі алгоритмів AES та Serpent, а також були показані практичні реалізації атак

на потокові (LILI-128, Toyocrypt та ін.) та блокові (спрощені варіанти AES, Camellia, KHAZAD, MISTY-1, KASUMI та ін.) шифри.

З метою спрощення процедури верифікації досліджуваних алгоритмів використовуються апаратно-програмні засоби криптоаналізу. Серед програмного забезпечення для алгебраїчного криптоаналізу варто виділити таке:

1. Система програм Ніколаса Куртуа [3], автора цього методу. Програмне забезпечення є закритим і орієнтованим на спрощені версії алгоритмів.

2. Система програм Мартіна Альбрехта [8] є розширенням для відкритого математичного пакета sage.

3. Система програм Мета Суса [9] містить багато утиліт для реалізації відповідного методу: cryptominisat2 (засіб для розв'язування рівнянь у кон'юнктивній нормальній формі), anf2cnf (конвертор з алгебраїчної нормальної в кон'юнктивну нормальну форму) тощо.

Це програмне забезпечення варто розглядати як прототипи, в яких реалізовано основні теоретичні положення автора методу, тому ці програмні продукти потребують доопрацювання та модифікації. Також варто зазначити, що програмне забезпечення п.2 і п.3 є відкритим і безкоштовним, що дає змогу скористатися ним під час розроблення власної криптоаналітичної системи.

Стосовно апаратних засобів, на думку авторів, доцільно використати для цього паралельну та розподілену комп'ютерну систему на основі GPU-кластера [10]. Проте автори розглядають можливості реалізації таких задач й у грід-середовищі [11].

Аналіз отриманих наукових результатів

Підвищити ефективність зазначених методів криптоаналізу та криптоаналітичних систем загалом можна:

1) зменшенням розмірності системи рівнянь і відповідно зменшенням трудомісткості алгоритму;

2) декомпозицією та подальшим розпаралеленням фрагментів обчислювальної задачі між обчислювальними засобами;

3) використанням спеціалізованих апаратних та програмних технологій, які б уможливили оптимізувати час виконання програм.

Перші два шляхи передбачають модифікацію алгоритмічного та математичного, а третій програмного забезпечення.

Модифікація програмного забезпечення полягає у розпаралеленні та векторизації деяких блоків криптоаналітичних алгоритмів. Розпаралелення полягає у паралельному опрацюванні окремими підпроцесами на окремих обчислювальних пристроях фрагментів обчислювальних задач алгоритму. Оскільки потокові шифри побудовані на використанні регістрів зсуву зі зворотними зв'язками, тобто йде опрацювання векторів даних, то доцільно здійснити векторизацію алгоритмів використанням векторних інструкцій сучасних процесорів, а саме: SSE, SSE2, AVX тощо. Автори здійснили модифікацію наведеного програмного забезпечення для алгебраїчного криптоаналізу потокових шифрів розпаралеленням та векторизацією фрагментів коду з метою реалізації апаратно-програмного комплексу для криптоаналізу.

Декомпозицію обчислювальної задачі планується здійснювати на етапах опрацювання вхідних даних, використовуючи декомпозицію за даними, та на етапі розв'язання системи рівнянь – шляхом використання функціональної декомпозиції. Під час створення програмної системи, з урахуванням архітектурних особливостей обчислювального GPU-кластера [10] будуть використані такі види паралелелізму:

- дрібнозернистий та середньозернистий – на рівні GPU-пристроїв, використовуючи технологію OpenCL;
- великозернистий – на рівні кластера або грід-системи, використовуючи технології MPI.

Висновки і перспективи подальших наукових розвідок

Розглянуто теоретичні аспекти криптоаналізу потокових шифрів. Наведено та здійснено короткий аналіз відомих методів та засобів криптоаналізу потокових шифрів. Сформульовано рекомендації щодо подальшого вдосконалення відомих криптоаналітичних методів.

Подальші наукові дослідження передбачають:

- розробку систем рівнянь у нормальній алгебраїчній формі, які б описували спрощені аналоги вітчизняних алгоритмів шифрування, з метою їх криптоаналітичного дослідження методами алгебраїчного криптоаналізу;
- модифікацію існуючого програмного забезпечення для його виконання у паралельних та розподілених обчислювальних системах, зокрема на GPU-кластерах та в грід-системах;
- тестування, відлагодження й коригування існуючого програмного забезпечення з урахуванням недоліків його роботи;
- створення комплексної системи для криптоаналізу потокових шифрів з урахуванням вимог організацій стандартизації.

1. Network Taps. Net Optics. Inc. – [Електронний ресурс]. – Режим доступу: URL: http://www.netoptics.com/products/network-taps. – Назва з екрану. 2. Golic J., Cryptanalysis of Alleged A5 Stream Cipher, proceedings of EUROCRYPT'97, LNCS 1233. – P. 239–255, Springer-Verlag 1997. 3. Courtois N., Klimov A., Patarin J, Shamir A. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations B.Prenell (Ed.): EUROCRYPT 2000, LNCS 1807. – P. 392–407, 2000. Springer-Verlag Berlin Heidelberg 2000. 4. Heys H.M. and Tavares S.E. The design of substitution-permutation networks resistant to differential and linear cryptanalysis. In CCS '94: Proceedings of the 2nd ACM Conference on Computer and communications security, New York, NY, USA, 1994. – P. 148–155 ACM Press. 5. Johannes Buchmann, Jintai Ding, Mohamed Saied Emam Mohamed, Wael Said Abd Elmageed Mohamed MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis. Dagstuhl Seminar Proceedings 09031. Symmetric Cryptography. – [Електронний ресурс]. – Режим доступу: URL: http://drops.dagstuhl.de/opus/volltexte/2009/1945. – Назва з екрана. 6. Nicolas T. Courtois, Sean O'Neil and Jean-Jacques Quisquater: Practical Algebraic Attacks on the Hitag2 Stream Cipher, In 12th Information Security Conference, ISC 2009, Pisa, Italy 7–9 September 2009, Springer LNCS 5735. – P. 167–176. 7. N. Ferguson, R. Shroeppel, and D. Whiting, A simple algebraic representation of the AES, Selected Areas in Cryptography, SAC 2001, S. Vaudenay and A.M. Youssef (editors), Lecture Notes in Computer Science, vol. 2259, Springer–Verlag, Berlin – New York, 2001. – P. 103–111. 8. Martin Albrecht source code for algebraic attacks. – [Електронний ресурс]. – Режим доступу: URL: https://bitbucket.org/malb/algebraic_attacks. – Назва з екрана. 9. CryptoMiniSat2. – [Електронний ресурс]. – Режим доступу: URL: http://www.msoos.org/cryptominisat2./ – Назва з екрана. 10. Загородна Н.В., Лупенко С.А. Луцків А.М. Обґрунтування вибору доступних програмно-апаратних засобів високопродуктивних обчислювальних систем для задач криптоаналізу // Електроніка та системи управління-2011.– К.: НАУ, 2011. – №1(27). – С. 42–50. 11. Загородна Н.В., Лупенко С.А. Луцків А.М. Реалізація сучасних криптоаналітичних методів у обчислювальному грід-середовищі на основі кластерних архітектур // Електроніка та системи управління-2011. – К.: НАУ, 2011. – №3(29). – С. 5–15.