УДК: 517.9:519.8

Антонюк А. О., здобувачка вищої освіти,
Луценко А. В., д-р філософії з математики,
в. о. завідувача кафедри прикладної математики та кібербезпеки,
Донецький національний університет імені Василя Стуса

МАТЕМАТИЧНИЙ АНАЛІЗ ЯК МІСТ МІЖ ТЕОРІЄЮ І ПРАКТИКОЮ КРИПТОАНАЛІЗУ

Анотація. Робота досліджує ключову роль математичного аналізу як сполучної ланки між теоретичними основами криптографії та практичними методами криптоаналізу. Проведено огляд сучасних підходів: алгебраїчних, ґраткових, статистичних. Показано, як теоретичні концепції реалізуються в практичних атаках через спеціалізовані солвери та апаратне прискорення. Визначено виклики масштабованості та перспективи розвитку міждисциплінарних методів.

Ключові слова: криптоаналіз, математичний аналіз, алгебраїчні атаки, ґраткові методи, статистичний аналіз.

Вступ. Криптоаналіз як наука про дослідження стійкості криптографічних систем базується на глибокій взаємодії між математичною теорією та практичною реалізацією атак. Математичний аналіз виступає критично важливим мостом, що дає змогу перетворювати абстрактні теоретичні концепції на конкретні алгоритми та методи, здатні ефективно аналізувати реальні криптографічні системи.

Сучасний криптоаналіз характеризується конвергенцією різноманітних математичних дисциплін – від класичної алгебри та теорії чисел до сучасних методів машинного навчання та інформаційної теорії. Ця міждисциплінарність створює унікальні можливості для розробки нових підходів до аналізу криптографічних примітивів, але водночас ставить нові виклики щодо інтеграції різних математичних методів у єдині практичні рішення [1].

Метою роботи є систематичний аналіз ролі математичних методів у забезпеченні зв’язку між теоретичними основами криптографії та практичними техніками криптоаналізу, а також визначення перспективних напрямів розвитку цієї галузі.

Основний текст

Основні математичні методи в криптоаналізі. Алгебраїчні методи криптоаналізу базуються на представленні криптографічних примітивів, як-от S-блоки, у вигляді систем поліноміальних рівнянь над скінченними полями. Для розв’язання цих систем застосовуються потужні інструменти, зокрема алгоритми побудови баз Грьобнера, а також методи перетворення з алгебраїчної нормальної форми (ANF) до кон’юнктивної нормальної форми (CNF) для подальшої інтеграції з високоефективними SAT-солверами, що особливо важливо для аналізу багатовимірних криптосистем публічного ключа, як-от HFE [1; 2].

Ґраткові методи надають фундаментальний апарат для розв’язання задач пошуку коротких векторів, що є основою для атак на криптосистеми RSA з малими експонентами, схеми на основі задачі про приблизні спільні дільники (ACD) та системи повністю гомоморфного шифрування. Ключові алгоритми,

як-от LLL-редукція (Lenstra-Lenstra-Lovász) та вдосконалений BKZ-алгоритм (Block Korkine-Zolotarev), дають змогу ефективно будувати спеціалізовані ґратки для конкретних криптографічних завдань. Метод Howgrave-Graham демонструє, як теоретичні результати геометрії чисел трансформуються в практичні алгоритми з чітко визначеною складністю [2; 3].

Статистичні методи охоплюють класичні підходи, зокрема диференціальний та лінійний криптоаналіз, а також сучасні техніки, як-от бумеранг-атаки та інтегральний криптоаналіз. Вони ґрунтуються на аналізі ймовірностей диференціалів, лінійних апроксимаціях, кореляційних атаках на потокові шифри та ретельному статистичному тестуванні випадковості. Ефективність цих методів підтверджується експериментально, як, наприклад, у випадку множинної диференціальної атаки на алгоритм PRESENT [3].

Перетворення теорії в практику. Критичним етапом у криптоаналізі є перехід від теоретичних моделей до практичних атак, що реалізується через три взаємопов'язані стадії. Перша фаза – моделювання та формалізація – полягає у створенні адекватної математичної моделі криптографічного примітиву. Алгебраїчне моделювання передбачає представлення операцій шифрування у вигляді систем поліноміальних рівнянь з оптимальним вибором математичного представлення (ANF, CNF, поліноміальні кільця) та з урахуванням структурних особливостей алгоритму. Паралельно здійснюється ґраткове моделювання з побудовою відповідної ґратки для числової задачі, оцінкою її розмірності та детермінанта, вибором базису та стратегії редукції.

Друга фаза – алгоритмічна реалізація – включає ретельний вибір та оптимізацію обчислювальних інструментів. Використовуються спеціалізовані SAT-солвери для криптографічних задач, реалізації алгоритмів ґраткової редукції (LLL, BKZ) та інтегровані системи для гібридних атак. Чисельні методи застосовуються для перетворення дискретних задач у континуальні з подальшим використанням чисельних оптимізаторів, обробкою нестабільності та локальних мінімумів, а також реалізацією гібридних підходів, що поєднують дискретні та континуальні методи [4].

Третя фаза – інженерна оптимізація – забезпечує практичну ефективність через апаратне прискорення з використанням GPU для паралельних обчислень, спеціалізованих FPGA-реалізацій та кластерних обчислень для великомасштабних атак. Оптимізація алгоритмів досягається застосуванням евристик для скорочення простору пошуку, попередньої обробки даних та гібридних підходів, що інтегрують різні математичні методи для досягнення максимальної ефективності криптоаналітичних атак [5].

Конкретні приклади успішних атак. Алгебраїчні методи продемонстрували значний успіх у криптоаналізі багатовимірних криптосистем публічного ключа, зокрема HFE. Застосування алгоритмів побудови баз Грьобнера дало змогу ефективно знаходити прообрази хеш-функцій та відновлювати секретні ключі з практичною складністю, значно нижчою за повний перебір. Були реалізовані практичні атаки на параметри HFE розміром до 80 біт, розроблені покращені алгоритми для систем MQ та виявлені критичні вразливості в комерційних реалізаціях цих криптосистем [1].

Ґраткові методи забезпечили прорив у криптоаналізі RSA з малими експонентами та криптосистем на основі приблизних спільних дільників (ACD). Значне покращення теоретичних оцінок похибок та розробка високоефективних алгоритмів дали змогу успішно атакувати параметри, які раніше вважалися абсолютно безпечними. Серед ключових досягнень – практичні атаки на RSA з експонентами e = 3,65537, криптоаналіз схем повністю гомоморфного шифрування (FHE) з недостатньо великими параметрами шуму, а також розробка оптимізованих алгоритмів для різних варіантів задач ACD [2; 3].

Висновки. Дослідження показало, що ефективний сучасний криптоаналіз базується на конвергенції різноманітних математичних дисциплін – від класичної алгебри та теорії чисел до сучасних методів машинного навчання й інформаційної теорії.

Перспективи подальших досліджень пов’язані з розвитком гібридних методів, що поєднують переваги різних математичних підходів. Зокрема, перспективними є: інтеграція методів машинного навчання для евристичної оптимізації алгебраїчних та ґраткових атак; розробка квантово-стійких алгоритмів криптоаналізу на основі теорії ґраток, а також дослідження можливості застосування методів топологічного аналізу даних для виявлення слабких місць у криптографічних примітивах.

Список використаних джерел

1. Bard G. V. The Quadratic Sieve. Algebraic Cryptanalysis. Boston, MA, 2009. P. 159–183. DOI: 10.1007/978-0-387-88757-9_10.

2. Yang N., Tang C., He D. A Lightweight Certificateless Multi-User Matchmaking Encryption for Mobile Devices: Enhancing Security and Performance. *IEEE Transactions on Information Forensics and Security.* 2023. Vol. 19. P. 251–264. DOI: 10.1109/tifs.2023.3321961.

3. Cohn H., Heninger N. Approximate common divisors via lattices. *The Open Book Series.* 2013. Vol. 1, № 1. P. 271–293. DOI: 10.2140/obs.2013.1.271

4. Comparative Analysis of Automatic Exudate Detection between Machine Learning and Traditional Approaches / A. Sopharak et al. *IEICE Transactions on Information and Systems.* 2009. E92-D, № 11. P. 2264–2271. DOI: 10.1587/transinf.e92.d.2264.

5. Myasnikov A. G., Ushakov A. Random subgroups and analysis of the length-based and quotient attacks. *Journal of Mathematical Cryptology.* 2008. Vol. 2, № 1. P. 29–61. DOI: 10.1515/jmc.2008.003.