АЛГЕБРАЇЧНІ ВЛАСТИВОСТІ АЛГОРИТМУ ASCON У КОНТЕКСТІ КУБІЧНИХ АТАК

Руженцев В.І., Куценко Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток сучасних стандартів легковагової криптографії обумовлює необхідність поглибленого аналізу їхньої стійкості до алгебраїчних атак, які базуються на поданні криптографічних перетворень у вигляді систем булевих рівнянь над полем GF(2). Такий підхід дозволяє досліджувати криптографічні алгоритми з позицій їхньої внутрішньої алгебраїчної структури та виявляти потенційні вразливості, що не завжди очевидні при класичному аналізі. Особливу увагу в цьому контексті привертає алгоритм Ascon, який у 2023 році був стандартизований Національним інститутом стандартів і технологій США як базовий алгоритм легковагової криптографії

Алгоритм Ascon побудований на губчастій конструкції та використовує внутрішній стан фіксованого розміру, до якого послідовно застосовуються раундові перетворення. Кожен раунд включає додавання константи, нелінійне перетворення у вигляді 5-бітного S-блоку та лінійний дифузійний шар [1].

Нелінійний шар реалізується у bit-sliced формі, що забезпечує ефективність реалізації, але водночас обмежує початкову алгебраїчну складність функції. Лінійний шар, заснований на операціях XOR і циклічних зсувах, забезпечує швидке розповсюдження впливу окремих бітів по всьому стану. Така архітектура дозволяє досягти високої продуктивності, однак з точки зору алгебраїчного криптоаналізу вона створює передумови для побудови компактних поліноміальних моделей.

Алгебраїчне представлення алгоритму здійснюється через запис кожного вихідного біта як булевої функції від вхідних змінних у вигляді алгебраїчної нормальної форми. У цьому випадку функція описується поліномом над GF(2), а її складність визначається алгебраїчним ступенем, тобто максимальним ступенем мономів у цьому поліномі. Алгебраїчний ступінь є одним із ключових параметрів, що визначають стійкість до алгебраїчних атак. Для алгоритму Ascon характерно, що S-блоки мають обмежений розмір входу, що призводить до відносно низького початкового ступеня. У результаті після одного або декількох раундів ступінь функції зростає поступово, а не досягає максимального значення миттєво. Це явище є критично важливим, оскільки повільний ріст алгебраїчного ступеня створює передумови для застосування спеціалізованих методів криптоаналізу, зокрема кубічної атаки.

Кубічна атака (cube attack) належить до класу алгебраїчних атак і базується на аналізі багатовимірних булевих функцій шляхом варіювання підмножини їхніх змінних. Нехай криптографічний алгоритм задає функцію f (k,v), де k — секретний ключ, а v — набір відкритих або керованих змінних. Обирається підмножина змінних C={v1,v2,…,vt}, яка називається кубом, після чого виконується повний перебір усіх можливих значень цих змінних. Для кожної комбінації обчислюється значення функції, і результати підсумовуються за модулем два. У результаті отримується нова функція від ключа p(k)), яка називається суперполіномом.

Ключова властивість cube attack полягає в тому, що при певному виборі куба всі члени полінома, які містять хоча б одну змінну з куба у степені менше за максимальний, занулюються при підсумовуванні. У результаті залишається лише частина функції, яка залежить від змінних поза кубом, зокрема від бітів ключа. Якщо алгебраїчний ступінь функції обмежений, то існує можливість підібрати такий куб, для якого суперполіном буде або лінійною функцією від ключа, або функцією низького ступеня. Це дозволяє відновлювати ключ або його частини шляхом розв'язання значно спрощеної системи рівнянь [2].

Ефективність cube attack визначається кількома факторами. По-перше, це алгебраїчний ступінь функції: чим він нижчий, тим більша ймовірність існування корисних кубів. По-друге, важливу роль відіграє структура залежностей між змінними, яка визначає, які мономи залишаються після підсумовування. По-третє, критичним є вибір самого куба, оскільки від цього залежить форма суперполінома. У загальному випадку задача вибору куба є складною комбінаторною проблемою, що має експоненційну складність, однак на практиці можуть застосовуватися евристичні підходи, які дозволяють знаходити ефективні куби. Особливий інтерес становлять так звані high-dimensional cube атаки, в яких розмір куба є великим. Зі збільшенням розмірності куба зростає ймовірність того, що всі небажані мономи будуть занульовані, однак різко зростає обчислювальна складність атаки. Теоретично складність такої атаки становить 2t, де t - розмір куба. Проте важливо відзначити, що навіть при великих значеннях ttt можливе використання статистичних методів, які дозволяють оцінювати властивості суперполінома без повного перебору, що відкриває нові можливості для практичної реалізації атак. У контексті алгоритму Ascon cube attack є особливо релевантною через його алгебраїчну структуру. Обмежений алгебраїчний ступінь S-блоків та поступове зростання складності функції по раундах створюють умови, за яких для скорочених версій алгоритму можуть існувати куби, що призводять до інформативних суперполіномів. Це означає, що для певної кількості раундів можливе відновлення залежностей від ключа з меншою складністю, ніж це передбачено теоретичними оцінками.

Важливим аспектом є також те, що сучасні оцінки криптостійкості часто базуються на припущенні про повне насичення алгебраїчного ступеня після достатньої кількості раундів. Проте відсутність точних аналітичних результатів щодо швидкості цього насичення залишає відкритим питання про реальний запас стійкості алгоритму. У цьому контексті існує обґрунтоване припущення, що оцінки стійкості можуть бути завищеними, особливо для сценаріїв, де використовуються скорочені версії алгоритму або специфічні режими роботи. У рамках даного дослідження пропонується підхід до аналізу стійкості алгоритму Ascon, що базується на побудові його алгебраїчної моделі, дослідженні властивостей S-блоків та аналізі динаміки зростання алгебраїчного ступеня. Особлива увага приділяється дослідженню cube attack, включаючи аналіз умов її ефективності, та оцінки властивостей суперполіномів. Передбачається проведення експериментального аналізу для скорочених версій алгоритму з метою перевірки теоретичних висновків та оцінки практичної складності атаки [3].

У контексті cube-атак оцінка криптостійкості алгоритмів, зокрема Ascon, суттєво залежить від набору параметрів, які в класичних підходах часто інтерпретуються неточно або надто оптимістично. Cube attack ґрунтується на алгебраїчному представленні криптографічної функції у вигляді булевого полінома та використанні властивостей алгебраїчної нормальної форми (ANF), зокрема ефекту елімінування мономів при сумуванні по підмножинах змінних. У цьому контексті ключовими стають такі характеристики, як алгебраїчний степінь функції, розмір і структура cube, а також поведінка суперполіномів, які утворюються після сумування.

Одним із найбільш неточних показників у контексті cube attack є алгебраїчний ступінь функції як “гарантія стійкості”. У класичній інтерпретації вважається, що високий ступінь булевої функції автоматично ускладнює алгебраїчні атаки. Проте для cube attack цей показник є лише верхньою межею складності, оскільки атака експлуатує не загальний ступінь функції, а ступінь суперполінома, який може бути значно нижчим за глобальний алгебраїчний ступінь алгоритму. Таким чином, навіть функції з високим ступенем після достатньої кількості раундів можуть залишати локальні структури низького ступеня, що робить можливим побудову ефективних cube-атак, особливо для скорочених версій алгоритму.

У класичних моделях вважається, що після достатньої кількості ітерацій ступінь функції досягає максимального значення і подальші алгебраїчні атаки стають неефективними. Проте для cube attack критичною є не лише глобальна поведінка ступеня, а й локальні алгебраїчні структури, які можуть зберігатися навіть після досягнення високого ступеня. Це означає, що навіть “насичені” перетворення можуть залишати підструктури, придатні для побудови ефективних кубічних атак. Отримані результати свідчать про те, що алгебраїчні властивості алгоритму Ascon, зокрема обмежений ступінь нелінійних перетворень та його поступове зростання, можуть створювати передумови для застосування cube attack. Це підкреслює необхідність більш детального аналізу криптостійкості легковагових алгоритмів з урахуванням їхньої алгебраїчної структури та потенційних векторів атак.

Список літератури

1. Lightweight cryptography project of the American National Institute of Standards and Technology, 2015. Електронний ресурс. Режим доступу: https://csrc.nist.gov/projects/lightweight-cryptography

2. Lars R. Knudsen. Truncated and higher order differentials. In Bart Preneel, editor, Fast Software Encryption, pp. 196–211, Berlin, 1995. Springer Berlin Heidelberg. Електронний ресурс. Режим доступу: https://doi.org/10.1007/3-540-60590-8_16

3. Jules Baudrin, Anne Canteaut, and Léo Perrin. Practical cube attack against nonce misused Ascon. IACR Transactions on Symmetric Cryptology, 2022(4): pp. 120–144, Dec. 2022. Електронний ресурс. Режим доступу: https://doi.org/10.46586/tosc.v2022.i4.120-144

4. Cihangir Tezcan. Truncated, impossible, and improbable differential analysis of ascon. Cryptology ePrint Archive, Paper 2016/490, 2016. Електронний ресурс. Режим доступу: https://eprint.iacr.org/2016/490