Санкт-Петербургский государственный политехнический университет
кафедра ИБКС

Ростовцев Александр Григорьевич, alexander.rostovtsev@ibks.ftk.spbstu.ru
Мизюкин Алексей Вадимович

Системы разреженных булевых уравнений и алгебраические атаки

www.ssl.stu.neva.ru

Шифры и булевы уравнения (1)

Подробнее см. http://e-print.iacr.org./2012/151, журнал «Проблемы информационной безопасности. Компьютерные системы».

Кольцо полиномов Жегалкина КПЖ:

$\mathcal{G}_n[\mathbf{x}] = \mathbb{F}_2[\mathbf{x}]/\mathfrak{F}$, где $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathfrak{F} = (x_1^2 - x_1, \ldots, x_n^2 - x_n)$ – идеал, задающий простое поле.

Булево кольцо: $x^2 = x$ для всех x, коммутативно и имеет характеристику 2.

Конечное булево кольцо изоморфно КПЖ или его кольцу классов вычетов. Булево уравнение – полиномиальное уравнение в КПЖ. Решение булева уравнения = поиск нулей полинома.

Шифр $\mathbf{y} = C(\mathbf{x}, \mathbf{k})$ описывается как система полиномов из КПЖ. При известных $\mathbf{x}$, $\mathbf{y}$ вскрытие ключа сводится к решению системы булевых уравнений.

Переменные – разряды ключа и промежуточных текстов (10-раундовый AES – 1280 переменных).

Шифр быстрый $\Rightarrow$ уравнения разрежены (каждый полином короткий и содержит небольшое число переменных).

Шифры и булевы уравнения (2)

Алгебраическая атака – решение систем булевых уравнений (поиск общих нулей полиномов).

Y. Crama, P. Hammer. Boolean Functions: Theory, Algorithms and Applications (Cambridge Press, 2011, 711 p.). Алгоритмов много, но практических результатов нет. По-видимому, аппарат булевых функций – не лучший для алгебраических атак.

Методы решения систем булевых уравнений: Куртуа (XL), Фужер (базисы Гребнера БГ), Ву (характеристические множества), метод результантов, метод исключения переменных, …, метод Семаева (согласование и склейка) работает с таблицами, оптимизация проблематична.

Куртуа: пример успешной атаки на шифр, где каждое нелинейное уравнение содержит единственное нелинейное слагаемое – степени 2 (трехбитовая подстановка).

Методы Куртуа, Фужера, Ву, результантов, исключения переменных полиномиально сводятся к вычислению БГ. Емкостная сложность практически экспоненциальная.

Алгебраическая геометрия и алгебраические атаки

Алгебраическая геометрия занимается решением систем полиномиальных уравнений над полями (классическая алгебраическая геометрия) и над кольцами (теория схем).

Эллиптические кривые, алгебраические кривые в криптографии с открытым ключом – объекты алгебраической геометрии.

Шифр описывается системой полиномиальных уравнений и тоже является объектом алгебраической геометрии.

Алгебраическая геометрия: глубокая развитая теория и слабые вычислительные методы (быстро развиваются в последние годы).

В симметричной криптографии растет использование методов алгебраической геометрии (Франция, Германия, КНР). Есть тенденция к смещению математической подготовки криптографов в сторону алгебраической геометрии. На кафедре ИБКС СПбГПУ курс алгебраической геометрии читается около 20 лет и постоянно развивается.

Идеалы и многообразия (1)

Аффинное пространство $\mathbb{A}^n(K)$ – множество наборов n координат из K.

Идеал $(f_1, \ldots, f_k)$ кольца полиномов $K[\mathbf{x}]$ – множество полиномов вида $\{K[\mathbf{x}]f_1 + \ldots + K[\mathbf{x}]f_k\}$. Идеалы допускают сложение, умножение.

Многообразие идеала – множество его общих нулей в аффинном пространстве. Радикал идеала – наибольший идеал с тем же многообразием.

Многообразие максимального идеала – точка.

Многообразие $V(S)$ n-битового отображения $\mathbf{y} = S(\mathbf{x})$ – 2^n точек с $2n$ координатами $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{y} = (y_1, \ldots, y_n)$. Подстановка – отображение.

Идеал отображения $\mathfrak{A}_S$ – множество неявных полиномов от $\mathbf{x}$, $\mathbf{y}$, обращающихся в 0 на многообразии отображения.

Координатное кольцо отображения – $\mathcal{G}_n[\mathbf{x}]/\mathfrak{A}_S$.

Идеалы и многообразия (2)

Обратные подстановки и возможно другие отображения, заданные переставленными переменными имеют одинаковые идеалы и многообразия (DES, ГОСТ-28147 от центробанка).

Как можно задать идеал подстановки шифра?

1. Набором n булевых функций $y_i = S_i(\mathbf{x})$ – неинтересно, так делают все.
2. Неявными полиномами минимальной степени (Куртуа, Фужер).
3. Цепочкой вложенных идеалов/многообразий (продолжая традиции Э. Нетер и Э. Артина, цепочки идеалов – основной аппарат современной алгебры).

Булевы идеалы и многообразия

Булевы идеалы радикальны и биективно соответствует булевым многообразиям – множествам общих нулей полиномов идеала.

Решение системы булевых уравнений – поиск многообразия (или его точки).

Мономиальный идеал задается мономами, биномиальный – биномами, триномиальный – триномами и т.д.

Куртуа: Число полиномов больше чем число переменных.

Фужер: решение системы – это вычисление базиса Гребнера в КПЖ как для целостного кольца, сизигии приводятся по модулю идеала $\mathfrak{F}$. (Куртуа – аналогичный метод).

Идеал подстановки AES задается 24 квадратными полиномами от 16 переменных.

Базисы Гребнера (1)

Вскрытие ключа вычислением базиса Гребнера в $\mathcal{G}_n[\mathbf{x}]$ по Бухбергеру, Фужеру. Считаем, что ключ единственный.

1. Упорядочиваем переменные и мономы.
2. Для каждой пары полиномов из базиса идеала вычисляем сизигию (линейную комбинацию полиномов над множеством мономов) так, что сокращаются старшие мономы, и добавляем ее к базису идеала.
3. Удаляем лишние полиномы из базиса идеала.
4. Повторяем п. 2, 3 до тех пор, пока не останутся только биномы вида $(x_i + e_i)$ для переменных, задающих ключ. Ключ равен $(e_1, \ldots, e_n)$.

Сложность атаки обусловлена тем, что первоначальный и итоговый базисы заданы разреженными полиномами, но промежуточные результаты требуют экспоненциальной памяти.

Базисы Гребнера (2)

Исторически базисы Гребнера появились для деления полиномов нескольких переменных в целостных кольцах. Ненулевой остаток от деления двух полиномов зависит от способа упорядочения переменных.

Для деления в КПЖ БГ не нужны, это искусственное образование.

Основная идея: максимально уменьшить длину сизигий. Этому способствует увеличение числа полиномов в базисе идеала (сильный механизм) и уменьшение степени полиномов (слабый механизм).

Сизигия от полинома и бинома не длиннее полинома, длина сизигии от полинома и тринома увеличивается не более чем на 1.

Булевы идеалы и многообразия

Сумма идеалов: $\mathfrak{A} = (f_1, \ldots, f_m) \Leftrightarrow \mathfrak{A} = (f_1) \oplus \ldots \oplus (f_m)$.

Некоторые факты.

1. Кольцо $\mathcal{G}_n[\mathbf{x}]$ (КПЖ) – нетерово и артиново, размерности 0.
2. Идеалы допускают сложение $\oplus$ и умножение (= пересечение). По сложению и умножению идеалы образуют коммутативные моноиды.
3. Почти любой идеал можно задать суммой различного числа идеалов (существует однозначное разложение на простые множители и однозначное разложение на неприводимые слагаемые).
4. Группа автоморфизмов КПЖ состоит из перестановок простых идеалов. Все автоморфизмы КПЖ бирегулярны (задаются наборами полиномов).
5. Аффинная эквивалентность идеалов позволяет обобщить понятие дифференциала, линейной суммы с подстановок на идеалы и может быть использована в криптоанализе.

Деление полиномов Жегалкина

Деление идеалов $\mathfrak{B}$ на $\mathfrak{A}$ означает вычисление $\mathfrak{B}(\mathrm{mod}\ \mathfrak{A})$.

Факт. В КПЖ существует следующие виды деления с остатком:

(1) Полиномиальное (П) деление через базисы Гребнера (требует упорядочения переменных, используются в алгоритмах Бухбергера, Фужера);

(2) алгебро-геометрическое (АГ) деление через упорядоченность многообразий (не требует упорядочения переменных, его можно менять по ходу вычислений);

(3) а также множество промежуточных вариантов деления.

Много способов деления расширяет вычислительные возможности для получения короткого остатка от деления двух полиномов.

Булевы идеалы и многообразия (3)

Теорема 1. Если шифр задается биномиальным идеалом, то ключ вскрывается с полиномиальной сложностью вычислением базиса Гребнера (БГ).

Доказательство. Сизигия от пары биномов – бином.

Задача распознавания биномиальности идеала не решена [D. Eisenbud, B. Sturmfels. Binomial ideals, Duke math. J., 1996].

Предлагается: (1) задавать идеал короткими полиномами; (2) задавать идеал как цепочку вложенных идеалов.

Факт: чем больше число линейно независимых полиномов в базисе идеала, тем быстрее вычисляется БГ (избыточность полезна!).

Теорема 2. Для суммы идеалов имеем $\mathfrak{A} \oplus \mathfrak{B} = \mathfrak{A} \oplus (\mathfrak{B} (\mathrm{mod}\ \mathfrak{A}))$.

Следствие 3. Очередное булево уравнение можно рассматривать по модулю идеала, заданного предыдущими уравнениями, возможна рекурсия.

План алгебраической атаки

План алгебраической атаки. Исходный идеал $\mathfrak{A}$. Переменные – ключ и промежуточные тексты (AES 10 раундов – 1280 переменных).

1. Подготовка – разложение идеала в сумму $\mathfrak{A} = \mathfrak{I} \oplus \mathfrak{F} \oplus \mathfrak{B}$, $\mathfrak{B} = \mathfrak{A} \pmod{\mathfrak{I} \oplus \mathfrak{F}}$.
   Идеал $\mathfrak{I}$ задан короткими полиномами. Базис идеала $\mathfrak{B}$ короче и меньшей степени, чем базис идеала $\mathfrak{A}$.
   АГ-делением находим мономы $\mathfrak{Mon}$, биномы $\mathfrak{Bin} \pmod{\mathfrak{Mon}}$, триномы $\mathfrak{Trin}$ и т.д., обращающиеся в 0 на $V(\mathfrak{A})$. Полагаем $\mathfrak{I} = \mathfrak{Mon} \oplus \mathfrak{Bin} \oplus \mathfrak{Trin} \oplus \ldots$ Находим $\mathfrak{B} = \mathfrak{A} \pmod{\mathfrak{I} \oplus \mathfrak{F}}$. (Символьные пакеты MATHEMATICA, MAPLE работают плохо).
2. Собственно решение. Вычисляем БГ для идеала $\mathfrak{B}$ и рекурсивно поднимаем результат в предыдущее координатное кольцо (по аналогии с леммой Гензеля). Параллельным аппаратным вычислителем с комбинированным П- и АГ-делением «прореживаем» сизигии, удаляя те суммы, которые делятся на мономы, биномы, триномы, …. Деление может быть с остатком (из сизигии удаляется пара мономов, соответствующая триному, и добавляется недостающий моном из тринома). Парадокс: логика деления на триномы проще, чем на биномы.

Аффинная эквивалентность идеалов (1)

Предположение 4. Добавление к идеалу линейного уравнения несущественно изменяет сложность вычисления многообразия.

Если предположение 4 верно, то появляется инструмент уменьшения длины полиномов:

аффинная эквивалентность идеалов: $\mathfrak{A}(\mathbf{x}) \sim \mathfrak{B}(\mathbf{u})$, если $\mathbf{u} = L\mathbf{x} + \mathbf{c}$, L – обратимая матрица. Это обобщение аффинной эквивалентности подстановок, там матрица L блочно диагональная (аффинные отображения действуют только на вход или только на выход).

АЭИ позволяет определить понятие дифференциала и нелинейности подстановки для идеала.

Теорема 5. Аффинная эквивалентность идеалов сохраняет максимальные вероятности дифференциалов и нелинейности. Координатные кольца аффинно эквивалентных идеалов содержат одинаковое число аффинных полиномов.

Аффинная эквивалентность идеалов (2)

Эксперимент: аффинная эквивалентность идеала 4-битовой подстановки шифра SAES (simplified AES – общепринятый шифр). Многообразие: (09,14,2a,3b,4d,51,68,75,86,92,a0,b3,cc,de,ef,f7).

Нелинейность 4, вероятности дифференциалов $\leq 0{,}25$.

Главный идеал подстановки – длина 107. Задается триномами с точностью 0,52 и квадриномами с точностью 0,53.

Аффинно эквивалентный главный идеал не соответствует никакому отображению, имеет длину 14 и многообразие (1f,5f,6d,6f,9f,af,b9,ba,be,d3,d6,db,ed,f2,f3,fd). Задается триномами с точностью 0,76 и квадриномами с точностью 0,89.

Снижение средней степени мономов в базисе идеала: $\mathfrak{Mon}$ – 5, $\mathfrak{Bin}$ – 3,6, $\mathfrak{Trin}$ – 2,6, $\mathfrak{Quad}$ – 1,5.

Решение систем булевых уравнений (1)

Решение системы по п. 2 возможно двумя методами: точное решение и приближенное (истинный ключ находится как наиболее вероятный, как в статистических атаках).

Факт: средняя степень полинома при задании идеала подстановки цепочкой идеалов (мономы, биномы (mod $\mathfrak{Mon}$), триномы (mod $\mathfrak{Mon} \oplus \mathfrak{Bin}$)), … падает, как и в методах решета.

Сложность алгебраической атаки субэкспоненциальна???

Приложения к AES. Идеал подстановки AES задается одним полиномом длины 25465, или 8 полиномами длины 111 – 146, или

704 мономами степени 7,2; 3650 биномами; …

Скорость роста длины сизигии значительно ниже чем в известных методах.

Точность приближения короткими полиномами заметно возрастает при использовании виртуальных изоморфизмов..

Решение систем булевых уравнений (2)

Использование только мономиального идеала для подстановки AES сокращает длину сизигии на 1/3 в расчете на один байт.

Еще один способ ускорения: виртуальные изоморфизмы.

Виртуальный изоморфизм AES из предыдущего доклада увеличивает базис мономиального идеала до 1144 (средняя степень 7,0) и сокращает длину сизигии вдвое в расчете на один байт.

КПЖ конечно, выигрыш в решающей степени зависит от того, насколько длина сизигии приблизится к фундаментальному ограничению 2^(2^*n*), *n* – число переменных в идеале.

Нужно максимально снижать длину полиномов, как первоначальных, так и сизигий. Отсюда следует механизм прореживания сизигий, архитектура аппаратного вычислителя.