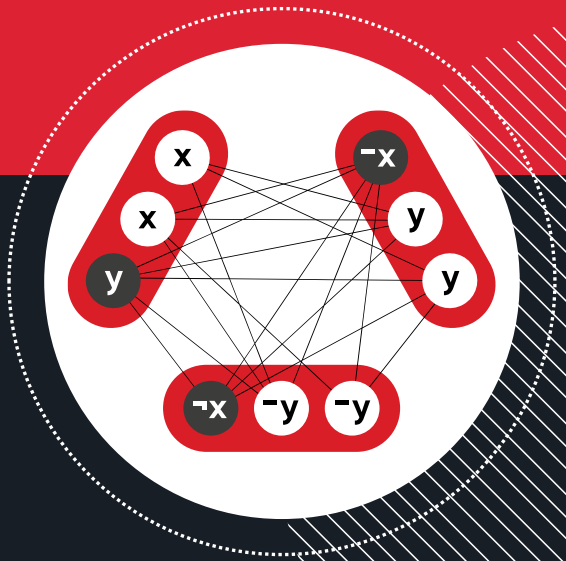
РУТОКЕН

конференция РусКрипто

Обзор применений SAT-решателей в целях криптоанализа симметричных криптографических алгоритмов



Марина Скоробогатова,
аналитик

Сергей Панасенко,
директор по научной работе

Задача выполнимости КНФ

Задача выполнимости (satisfiability problem): существует ли набор значений True/False для переменных $x_1, x_2, \ldots, x_n$ формулы $f(x_1, x_2, \ldots, x_n)$, при которых формула f истинна.

КНФ – конъюнкция дизъюнкций литералов (состоит из имён переменных, скобок и операций И, ИЛИ, НЕ

$\mathcal{F} = (x_1 \vee x_2) \wedge (x_1 \vee \neg x_2) \wedge (\neg x_1 \vee \neg x_2)$ — выполнима на наборе (1, 0)

Почему КНФ?

- Любая булева формула может быть приведена к КНФ
- Задача является NP-полной (теорема Кука)

Логический криптоанализ:
общая информация

- Термин введен в *F. Massacci, L. Marraro. Logical Cryptanalysis as a SAT Problem. Journal of Automated Reasoning, vol. 24, pp. 165-203, 2000*
- Применение ограничено быстрым ростом количества элементов формулы в зависимости от числа кодируемых в формуле преобразований (в частности, от количества раундов блочного шифра)
- Наиболее эффективен для решения частных задач в контексте применения других видов криптоанализа

Другое применение SAT-решателей:

- Разложение булевых матриц
- Минимизация продолжительности обработки задач (в том числе для процессоров)
- Автоматическая формальная верификация систем (model checking)
- Задачи на графах: соцсети, логистика и т.д.
- Решение игр (Судоку, Сапёр, анализ в шахматах)
- Кластеризация методом k-средних
- Автоматическая генерация тестов (ATPG)

Логический криптоанализ:
применение в криптографии

Анализ алгоритмов блочного симметричного шифрования:

- поиск секретного ключа (атаки на основе известного открытого текста);
- поиск классов слабых ключей (по отношению к дифференциальному или линейному криптоанализу);
- верификация ряда криптографических свойств блочных шифров (в частности, доказательство отсутствия слабых или универсальных ключей).

Анализ алгоритмов поточного шифрования и генераторов псевдослучайных последовательностей:

- поиск секретного ключа поточного шифра (атака на основе известного открытого текста);
- поиск начального заполнения генератора ключевого потока.

Анализ алгоритмов аутентифицированного шифрования:

- извлечение внутреннего состояния и раскрытие открытого текста;
- поиск секретного ключа;
- подделка аутентифицируемого сообщения.

Анализ функций хэширования:

- поиск прообразов;
- поиск коллизий (в том числе, путем поиска дифференциального пути с помощью SAT-решателя для последующего применения дифференциального криптоанализа).

Логический криптоанализ:
основная идея

- Описанные криптографические задачи сводятся к задачам о выполнимости КНФ, которые впоследствии решаются при помощи существующих реализаций SAT-решателей, умеющих находить наборы выполнимости заданных КНФ.
- Для этого биты открытого текста, ключа и шифротекста представим в виде последовательностей булевых переменных P, K и C. Каждая переменная принимает значения 1 (True) или 0 (False).
- Далее закодируем свойства криптографического алгоритма в виде булевой формулы E(P, K, C) такой, что E(P, K, C) = 1 $\Leftrightarrow$ C = E_k(P).
- Из выполнимости/не выполнимости формулы E(P, K, C) получаем информацию об исследуемом свойстве криптоалгоритма.

Анализ алгоритмов блочного симметричного шифрования: поиск секретного ключа

DES

Massacci F., Marraro L. Logical cryptanalysis as a SAT problem //Journal of Automated Reasoning. – 2000. – Т. 24. – С. 165-203.

Вычисление ключа шифрования на основе известного открытого текста для 3-раундового DES.

	Tableau	SATO	rel-SAT	
			С обучением	Без обучения
Раунды	2	3	3	
Блоки	4	8	8	
Успешность	100%	50%	100%	
Биты ключа	56	56	56	
Время	36.43	2192.73	75.03	164.792

SIMON32/64 (низкоресурсный)

Е. А. Маро, О. С. Заикин. Алгебраический криптоанализ 9 раундов низкоресурсного блочного шифра SIMON32/64. Труды XXII Международной конференции «Сибирская научная школа-семинар «Компьютерная безопасность и криптография» — Sibecrypt'23» им. Г. П. Агибалова, с. 65-70, 2023.

Вычисление ключа шифрования в предположении, что известны первые 16 бит ключа для 9 раундов SIMON-32/64.

SAT-кодировка 9-раундовой версии потребовала формирования 144 квадратичных уравнений со 176 переменными.

Прогноз 100% решения задачи для пары **случайных** открытых текстов:
~151ч для ключа (0xb2fe,0x7c97,0xa734,0x8a7f)
~94ч для ключа (0xe5e1,0x3e5c,0xfe34,0x7a47)
~73ч для ключа (0xd8a6,0x28f0,0x4c35,0xac81)

Анализ алгоритмов блочного симметричного шифрования: поиск слабых ключей

Поиск классов слабых ключей

F. Lafitte, J. Nakahara Jr., D. Van Heule. Applications of SAT Solvers in Cryptanalysis: Finding Weak Keys and Preimages. Journal on Satisfiability, Boolean Modeling and Computation, vol. 9, pp. 1-25, 2014.

Найдены классы слабых 512-битных ключей для 8.5-раундового блочного шифра WIDEA-4 и 1024-битных ключей для 8.5-раундового блочного шифра WIDEA-8.

Использование данных ключей существенно повышает вероятность успеха проведения атаки отличимости шифротекста (distinguishing attack) и атаки восстановления ключа (key recovery attack).

Доказано отсутствие классов слабых ключей для MESH-64(8).

Верификация криптографических свойств

F. Massacci, L. Marraro. Logical Cryptanalysis as a SAT Problem. Journal of Automated Reasoning, vol. 24, pp. 165-203, 2000.

Приведены примеры булевых формул для различных задач криптоанализа и верификации криптографических свойств блочных шифров (в частности, DES):

- кодирование сети Фейстеля
- кодирование перестановок
- кодирование S-боксов и др.

Анализ алгоритмов аутентифицированного шифрования

F. Lafitte, L. Lerman, O. Markowitch, D. Van Heule. SAT-based cryptanalysis of ACORN. Report 2016/521, Cryptology ePrint Archive, 2016.

Для версий v1, v2 AEAD-алгоритма ACORN успешно проведены следующие атаки с использованием SAT-решателя Cryptominisat:

- извлечение внутреннего состояния (state recovery attack)
- получение секретного ключа по внутреннему состоянию и открытому тексту (key recovery attack)
- нахождение коллизий — нахождение различных внутренних состояний, приводящих к одинаковому значению тэга (state collision attack)
- подделка аутентифицируемого сообщения (forgery attack)

Позже была описана 3 версия алгоритма ACORN, для которой данные атаки невыполнимы:

ACORN: A Lightweight Authenticated Cipher (v3). Designer and Submitter: Hongjun Wu, Division of Mathematical Sciences Nanyang Technological, University 2016.09.15

Анализ алгоритмов поточного шифрования и ГПСЧ

О. Заикин. SAT-криптоанализ криптографических хэш-функций и поточных шифров. Лекция в БФУ им. И. Канта, 2023.

Атаки на генератор ключевого потока A5/1 (используется для шифрования трафика в стандарте мобильной связи GSM):

- поиск секретного ключа поточного шифра
- поиск начального заполнения генератора

Для определения начального заполнения ключевого потока при известных значениях 31 из 64 битов внутреннего состояния с помощью модифицированного SAT-решателя Minisat-C достаточно 114 бит ключевого потока. Решение задачи занимает 0.2 секунды.

Анализ хэш-функций: поиск прообраза

SHA-1

Motara Y. M., Irwin B. V. W. SHA-1, SAT-solving, and CNF. – 2017.

Нахождение прообраза для полнораундовой хэш-функции SHA-1, имеющей до 20 свободных битов (остальные биты зафиксированы)

Свободных битов	SAT-решатель	Время (с)
16	Glucose	135.6
	Plingeling	25.8
	CryptoMiniSat	256.1
18	Glucose	403.6
	Plingeling	82.7
20	Glucose	227.8
>20	Слишком длинная КНФ	

РусКрипто'2019 (Маршалко, Мхитарян): поиск прообраза для 2-раундовой функции Стрибог с 20 свободными битами.

KECCAK

Morawiecki P., Srebrny M. A SAT-based preimage analysis of reduced Keccak hash functions //Information Processing Letters. – 2013. – Т. 113. – №. 10-11. – С. 392-397

- Найдены прообразы для 3-раундовой хэш-функции KECCAK.
- Показано, что полнораундовая хэш-функция KECCAK не подвержена атакам поиска прообраза.
- Для построения КНФ была использована утилита CryptLogVer.

Функция	Раундов	Размер сообщения (бит)	Размер хэша (бит)	Время (с)	
				SAT-решатель	Брут-форс
KECAAK[1024, 576]	3	24	1024	2^{0}	2^{1}
KECAAK[1024, 576]	3	32	1024	$2^{3,3}$	2^{9}
KECAAK[1024, 576]	3	40	1024	$2^{10,8}$	2^{17}
KECAAK[120,80]	3	24	80	$2^{2,5}$	$2^{-2,9}$
KECAAK[120,80]	3	32	80	$2^{5,7}$	2^{5}
KECAAK[120,80]	3	40	80	$2^{15,7}$	2^{13}

Анализ хэш-функций: поиск прообраза

В.В.Давыдов и др. SAT-криптоанализ криптографических хэш-функций BLAKE и GROESTL. // Летняя школа-конференция «Криптография и информационная безопасность» 2023. Сборник тезисов, с. 59-65

- 12-ядерный процессор AMD Ryzen 3900X
- Версия CBMC — 5.89

BLAKE-256

Число раундов	Время нахождения прообраза (с)	
	Нулевой хэш, 256 бит	Единичный хэш, 256 бит
8/64	0.51	0.29
9/64	21 596	2 133
10/64	8 798	27 089
11/64	20 004	2 281
12/64	11 654	Не решено
13/64	Не решено	Не решено

- Версия kissat — 3.0
- Для каждой КНФ запускался kissat на 1 ядре из 12

GROESTL

Число подраундов перестановок	Время нахождения прообраза (с)	
	Нулевой хэш, 256 бит	Единичный хэш, 256 бит
10/16, 4P6Q	94.14	50.72
10/16, 6P4Q	2.13	2.20
12/16, 8P4Q	3	2.88
10/64, 5P5Q	37 641	21 046
13/16, 8P5Q	27 077	11 780

Анализ хэш-функций: поиск коллизий

MD4/MD5

Mironov I., Zhang L. Applications of SAT solvers to cryptanalysis of hash functions //Theory and Applications of Satisfiability Testing-SAT 2006: 9th International Conference, Seattle, WA, USA, August 12-15, 2006. Proceedings 9. – Springer Berlin Heidelberg, 2006. – С. 102-115.

Найдены коллизии для полнораундовой хэш-функции MD4, 46-раундовой MD5, 35-раундовой SHA-0. Время поиска коллизии для полнораундового MD5 (для ПК 32 GHz PIV, 1Gb RAM) может достигать порядка 100 часов.

Хэш-функция	Всего раундов	Модификации		Формула		Время
		Wang et al, 2005	SAT	Переменных	Дизъюнктов	
MD4	48	48	48	53228	221440	~500с
MD5	64	22	46	89748	375176	<15м
SHA-0	80	20	35	114809	486185	<15м

SHA-1

О. Заикин. SAT-криптоанализ криптографических хэш-функций и поточных шифров. Лекция в БФУ им. И. Канта, 2023.

На основе атаки, описанной в *Stevens M. «New collision attacks on SHA-1 based on optimal joint local-collision analysis» (2013)* найдены коллизии для полнораундовой хэш-функции SHA-1.

SAT-решатели: неполные алгоритмы

Осуществляют поиск выполняющего набора неполным перебором пространства возможных решений.
В основном используют локальный поиск (local search).

\+ Приложение к другим задачам (MAXSAT)
\+ Быстрая скорость работы
— Могут доказать только выполнимость

Selman B., Leveque H., Mitchell D. A new method for solving hard satisfiability problems //Proceedings of the tenth national conference on artificial intelligence (AAAI-92). – 1992. – С. 440-446.

McAllester D. et al. Evidence for invariants in local search //AAAI/IAAI. – 1997. – С. 321-326.

GSAT — основан на стохастическом локальном поиске; при обращении переменной вносится изменение, минимизирующее количество невыполненных дизъюнктов в новой формуле (с некоторой вероятностью переменная выбирается случайно).

WalkSAT — при обращении переменной случайно выбирается дизъюнкт, который невыполним для данного значения переменной. Внутри дизъюнкта переменная выбирается с учётом рейтинга (рейтинг переменной равен числу дизъюнктов, для которых нарушается выполнимость при изменении данной переменной).

SAT-решатели: полные алгоритмы

Выполняют полный перебор. В отличие от неполных алгоритмов осуществляют **доказательство невыполнимости,** имеющее прикладное значение при верификации схем и автоматическом доказательстве теорем.

DPLL (Davis–Putnam–Logemann–Loveland)

Davis M., Logemann G., Loveland D. A machine program for theorem-proving //Communications of the ACM. – 1962. – Т. 5. – №. 7. – С. 394-397.

- GRASP
- SATO
- Chaff

CDCL (conflict-driven clause learning)

Silva J. P. M., Sakallah K. A. GRASP-a new search algorithm for satisfiability //Proceedings of International Conference on Computer Aided Design. – IEEE, 1996. – С. 220-227.

Look-ahead

Freeman J. W. Improvements to propositional satisfiability search algorithms. – University of Pennsylvania, 1995.

SAT-решатели: применение

Local search based	CDCL	Look-ahead
Хорошие результаты на случайных выполнимых 3-КНФ	Хорошие результаты на индустриальных КНФ	Хорошие результаты на невыполнимых КНФ
• GSAT • WalkSAT • CPSolver • Stochastic Local Search Based CSP Solver • SATenstein	• Cryptominisat • Minisat • zChaff • Glucose • kissat	• POSIT • Tableau • rel_sat • OKsolver • march

Подведем итоги

1. SAT-криптоанализ показал себя эффективным методом анализа симметричных криптографических примитивов.
К настоящему моменту он был успешно применен для решения различных задач по криптоанализу хэш-функций и блочных/потоковых шифров.

2. SAT-задачи могут быть использованы также для доказательства определенных свойств криптографических алгоритмов.

3. Для решения SAT-задач применяется хорошо изученный алгоритмический аппарат, позволяющий, в числе прочего, автоматизировать и распараллеливать решение задач по криптоанализу.

4. Основным фактором, ограничивающим применение SAT-криптоанализа, является быстрый рост количества элементов формулы в зависимости от числа кодируемых в формуле преобразований (в частности, от количества раундов криптоалгоритма)

5. Тем не менее, алгоритмы решения SAT-задач активно развиваются, можно ожидать в ближайшем будущем достижения новых значительных результатов с помощью SAT-криптоанализа.

Вопросы

Контактная информация

Марина Скоробогатова

sma@aktiv-company.ru
info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 996432-0421


30
КОМПАНИЯ
АКТИВ