УДК 519.719.2

ОБЗОР АТАК НА AES-128: К ПЯТНАДЦАТИЛЕТИЮ СТАНДАРТА AES

К. Д. Жуков

Лаборатория ТВП, г. Москва, Россия

Представлен обзор работ, опубликованных до 2016 г. и посвящённых криптоанализу алгоритма AES-128 (Advanced Encryption Standard). Перечислены основные криптографические методы, используемые при анализе AES. Приведены сложностные характеристики 88 атак на редуцированные варианты алгоритма AES-128. Указано необходимое для проведения атак количество известных пар шифрованных и открытых текстов с условиями на них. В поле зрения не попали атаки по побочным каналам и атаки с ограничением на используемые ключи.

Ключевые слова: *AES, Advanced Encryption Standard, методы дешифрования.*

DOI 10.17223/20710410/35/5

OVERVIEW OF ATTACKS ON AES-128: TO THE 15^{TH} ANNIVERSARY OF AES

K. D. Zhukov

TVP Laboratory, Moscow, Russia

E-mail: zhukov_kirill@bk.ru

This overview covers attacks on the reduced AES-128 published up to the end of 2016. We enumerate main cryptographic methods used in cryptanalysis of AES. We also tabulate the complexity characteristics of 88 attacks on the reduced AES-128 including the number and peculiarities of necessary plaintexts and ciphertexts. Side-channel attacks and related key attacks are out of the overview scope.

Keywords: *AES, Advanced Encryption Standard, key-recovery attack.*

Введение

В 1998 г. была опубликована схема блочного шифра Rijndael. С тех пор начался его интенсивный криптоанализ, который ещё больше усилился с принятием алгоритма в качестве американского стандарта шифрования AES [1]. За 15 лет опубликовано более ста печатных работ, посвящённых анализу Rijndael. Первая атака, теоретически понижающая стойкость AES, опубликована лишь в 2011 г. [2], спустя 10 лет после публикации стандарта. При этом понижение стойкости составило не более чем три двоичных порядка.

В общем случае под атаками на систему шифрования понимаются не только методы дешифрования. Например, в литературе изучается задача идентификации AES [3, 4]. В некоторых случаях на основе методов идентификации формулируются методы дешифрования. Далее сосредоточимся на работах, содержащих методы дешифрования.

Можно выделить три основных предположения криптоанализа, в рамках которых проводятся атаки на AES:

— анализ видоизменённой схемы (например, снижение числа раундов);
— использование дополнительной информации (например, утечка по побочным каналам, внесение искажений);
— специфические условия эксплуатации (например, подобранные открытые или шифрованные тексты, связанные ключи).

Данный обзор посвящен атакам на AES с уменьшенным числом раундов. При анализе редуцированных алгоритмов наблюдаются два подхода. Первый заключается в теоретическом понижении стойкости (по сравнению с методом тотального опробования) редуцированной схемы. Второй подход нацелен на построение практических атак на редуцированные версии алгоритма. Два подхода в определённой степени независимы: атаки, понижающие стойкость большего числа раундов, могут не улучшать атак на малое число раундов.

1. Алгоритм AES и способы построения редуцированных схем

Описанию алгоритма AES и используемому в нём математическому аппарату посвящена работа [5]. Ниже приводится краткая схема шифра.

Алгоритм AES представляет собой блочный шифр с длиной блока 128 битов (16 байтов) и с тремя возможными длинами ключей — 128, 192 и 256 битов. Блок шифра (промежуточное состояние) представляют в виде квадратной матрицы над полем $\mathrm{GF}(2^8)$ размера 4. Каждый элемент записывается одним байтом. Алгоритм реализуется итеративно несколькими раундами, которые состоят из следующих преобразований:

— `SubBytes (SB)` — применение одного и того же обратимого преобразования (S-блока) ко всем 16 байтам промежуточного состояния шифра;
— `ShiftRows (SR)` — циклический сдвиг каждой строки промежуточного состояния шифра (i-я строка сдвигается влево на i байтов, $i = 1, 2, 3, 4$);
— `MixColumns (MC)` — умножение слева каждого столбца промежуточного состояния на постоянную квадратную матрицу над $\mathrm{GF}(2^8)$ порядка 4;
— `AddRoundKey (ARK)` — побитовое сложение с раундовым ключом.

На первом раунде производится операция `AddRoundKey` с использованием дополнительного «отбеливающего» (*whitening*) ключа, а на последнем раунде отбрасывается операция `MixColumns`. Количество раундов зависит от длины используемого ключа: 10 раундов для 128-битового ключа, 12 раундов — для 192-битового и 14 раундов — для 256-битового ключа. Три варианта алгоритма AES обозначаются AES-128, AES-192 и AES-256 соответственно.

В работе [6] отмечается, что при одном и том же количестве раунодв AES стойкость итеративной схемы может существенно зависеть от наличия операции `MixColumns` на последнем раунде. Большинство известных атак на редуцированные версии AES сделаны в предположении, что на последнем раунде операция `MixColumns` не производится.

Однозначного определения редуцированного шифра AES нет даже у создателей стандарта. В исходной работе [7] редуцированные варианты AES, так же как и полный AES, не содержат операции `MixColumns` на последнем раунде шифрования. Одновременно с этим, при анализе редуцированного шифра в работе [8] операция `MixColumns` включается в последний раунд.

В [9] с помощью аппарата базисов Гребнера анализируются редуцированные схемы, в которых уменьшается количество строк (столбцов) в прямоугольном представлении промежуточного блока шифра, а также байты заменяются полубайтами. Такие редукции далее не рассматриваются.

Под атаками на AES будем понимать, в том числе, атаки на редуцированные варианты AES. Говоря об атаках на k раундов AES, будем предполагать, что на последнем раунде операция `MixColumns` не применяется. В противном случае будем говорить об атаках на k полных раундов AES.

2. Модели проведения атак на AES

Под моделью проведения атаки понимаются условия, в которых возможно реализовать атаку, а точнее, какие данные о работе шифра доступны криптоаналитику. В худшем случае наблюдателю доступны только шифрованные тексты на некоторых случайных ключах. В такой строгой модели формулирование атак затруднительно. Стойкость AES исследуется, как правило, в моделях из трёх основных классов: общие модели, модели с утечками по побочным каналам и модели с зависимыми ключами.

2.1. Общие модели

В общих моделях предполагается, что криптоаналитику известно некоторое количество пар открытых и соответствующих им шифрованных текстов. В классической постановке на открытые и шифрованные тексты не накладывается никаких ограничений. Наибольшее число атак на AES сделано в предположении, что открытые тексты, для которых известен результат шифрования, подобраны некоторым специальным образом. Реже встречаются атаки, в которых делается предположение о наличии открытых текстов для подобранных специальным образом шифрованных текстов.

В криптоанализе блочных шифров исследуются модели с адаптивно подбираемыми открытыми или шифрованными текстами [10]. Однако автор таких атак на AES не знает.

В работе [11] рассматриваются модели открытых текстов с подобранными разностями (при этом сами открытые тексты неизвестны).

2.2. Модели с утечками по побочным каналам

В последнее время становится популярным криптоанализ с использованием побочных каналов информации (*side-channel attacks*). Такую тенденцию можно объяснить двумя причинами. С одной стороны, с развитием технической базы атаки с использованием побочных каналов кажутся всё более и более реалистичными с точки зрения их реализации на практике. С другой стороны, при синтезе шифров такие атаки редко учитываются, а следовательно, у криптоаналитиков появляется возможность существенно понизить стойкость алгоритмов при некоторых благоприятных условиях.

Криптоанализ AES с использованием побочных каналов утечки информации представлен такими направлениями, как атаки при наличии доступа в кэш-память процессора (*cache attacks* [12]), анализ энергопотребления (*power analysis* [13]) и анализ разностных искажений (*differential fault analysis* [14]). Последний предполагает наличие возможности активного вмешательства в процедуру шифрования.

В данном обзоре атаки по побочным каналам на AES не рассматриваются. Однако нужно отметить, что методы разностных искажений могут быть применимы для построения атак в общих моделях. В [11] показано, что методы разностных искажений и разностный криптоанализ тесно связаны. Внесение искажения перед первым раундом шифрования можно рассматривать как подобранную пару текстов с фиксированной разностью в общей модели.

2.3. Модели с зависимыми ключами

В моделях с зависимыми ключами (*related key attack*) считается, что криптоаналитику известно некоторое количество пар открытых и шифрованных текстов, полученных путём шифрования на ключах, связанных каким-либо соотношением.

Как правило, в данной модели строится атака на такую пару ключей K_1 и K_2, что $K_2 = K_1 \oplus C$, где C — заданная константа. Применительно к AES существуют атаки и для более сложных зависимостей. Например, в [15] исследуется случай $K_2 = F^{-1}(F(K_1) \oplus C)$, где отображение F представляет собой один раунд ключевого расписания AES-256 (*related subkey attack*). В данном обзоре атаки с зависимыми ключами не рассматриваются.

3. Некоторые математическим методы криптоанализа AES

Ниже перечислены несколько математических методов, используемых при анализе AES в общей модели. Для некоторых методов приводится краткая идея или основное свойства шифра, позволяющее применить метод. Отметим, что приводимый список не претендует на полноту и затрагивает наиболее популярные техники.

3.1. Разностный криптоанализ

В общем случае разностный метод не эффективен для практических атак на AES, так как уже для четырёх раундов максимальное разностное отклонение не больше 2^{-150}. Однако данный метод и его модификации применяются для теоретического понижения стойкости редуцированных версий алгоритма.

Метод запретных разностей

Метод запретных разностей (*impossible differentials*) основан на следующем свойстве алгоритма AES [16].

Свойство 1. Два открытых текста, отличающихся только в одном байте, не могут при шифровании четырьмя раундами AES перейти в шифртексты с совпадающими байтами под номерами 1, 6, 11 и 16.

Зачастую метод запретных разностей применяется вместе с методом «встреча посередине».

Метод усеченных разностей

Метод усечённых разностей (*truncated differentials*) предложен в [17] в 1995 г. В отличие от классического разностного криптоанализа, в методе исследуются разности не блоков, а только частей блоков. Атаки на AES с применением данного метода построены в [4].

Техника раннего обрыва

В [18] метод запретных разностей усовершенствован с использованием техники раннего обрыва (*early abort technique*), которая опирается на следующее свойство AES.

Свойство 2. Рассмотрим набор из всевозможных 4×255 промежуточных состояний шифра с ненулевым байтом в первой колонке. После последовательного применения преобразований $\mathtt{MC}^{-1}$ и $\mathtt{RC}^{-1}$ пара байтов под номерами 1 и 6 будет различна во всех 4×255 состояниях набора.

3.2. Политопный криптоанализ

Политопный криптоанализ появился в 2016 г. как обобщение разностного метода. В [19] с помощью метода запретных политопных переходов получены атаки на редуцированный AES.

3.3. Интегральный криптоанализ

Авторство интегрального криптоанализа принадлежит Л. Кнудсену. С помощью данного подхода изначально анализировался предшественник алгоритма Rijndael — блочный шифр Square [20]. Отсюда берёт название базовая атака интегрального криптоанализа применительно к анализу AES — атака «Квадрат».

Метод «Квадрат»

Метод основан на следующем свойстве блочного шифра AES [7].

Свойство 3. Рассмотрим набор из 256 открытых текстов, в которых на фиксированной позиции байты пробегают всевозможные 256 значений, а на остальных позициях во всех текстах байты одинаковы. После применения трёх раундов AES побитовая сумма всех полученных 256 шифртекстов равна 0.

Метод частичных сумм

В 2000 г. в [21] предложена модификация атаки «Квадрат», получившая название техники частичных сумм (*partial sums*), которая была затем улучшена в работе [22].

3.4. Метод цепочек подпространств

Метод цепочек подпространств (*subspace trail*) появился в 2016 г. [4] как обобщение известного метода инвариантных подпространств [23]. Для построения атак на AES метод комбинируется с вариациями разностного метода.

3.5. Метод «Биклик»

Метод «Биклик» впервые применён к анализу AES в 2011 г. [2] А. Богдановым, Д. Хорватовичем и К. Рехбергом. В настоящее время метод является самым сильным при анализе полнораундовых вариантов алгоритма AES.

3.6. Метод «встреча посередине»

Метод «встреча посередине» предлагает общий подход к анализу блочных шифров. Данная техника может применяться в совокупности с другими методами. В общем виде с методом можно ознакомиться, например, в [2, 24].

Использование метода «встреча посередине» на отдельных подэтапах восстановления ключа

В [25] показано, что применение метода «встреча посередине» позволяет сформулировать эффективные критерии отбраковки ложных вариантов ключа на определённых этапах его восстановления в редуцированном алгоритме AES.

Техника просеивания посередине

В 2013 г. французские математики предложили технику просеивания посередине (*sieve-in-the-middle*) [24]. Техника получила развитие в работе [26], где применяется вместе с методом «Биклик». Отметим, что похожая техника зависящего от ключа просеивания (*key-dependent sieve*) в менее общем виде сформулирована независимо китайскими учеными [27].

Метод построения коллизий

В 1999 г. в [28] впервые было предложено использовать методы идентификации блочного шифра Rijndael для построения атак на редуцированные версии алгоритма. Эти идеи получили развитие в работах азиатских ученых [29 – 32].

3.7. Автоматизированный поиск алгебраических соотношений и разностных характеристик

Французские криптографы разрабатывают автоматизированные (реализуемые с помощью компьютера) методы поиска алгебраических соотношений, связывающих биты открытого и шифрованного текстов с битами ключа [33], соотношений между битами раундовых ключей [34], а также поиска разностных характеристик для связанных ключей [35]

4. Обзор атак на редуцированный AES-128 в общей модели

На момент составления данного обзора опубликована не одна сотня атак на AES-128, AES-192 и AES-256. В таблице приводятся атаки только на редуцированный AES-128 в классической модели (атаки по побочным каналам и в модели с зависимыми ключами не рассматриваются). Общее количество атак на редуцированный AES-128 с учётом различных моделей приблизительно вдвое больше, чем указано в таблице.

В первом столбце таблицы для дальнейших ссылок указан порядковый номер атаки. Атаки упорядочены по количеству анализируемых раундов AES-128 (второй столбец). Атаки на одинаковое количество раундов перечислены в произвольном (не хронологическом) порядке.

Третий столбец содержит индикатор присутствия операции `MixColumns` на последнем раунде рассматриваемого варианта редуцированного шифра. Присутствие операции обозначается символом ✓, а отсутствие — символом ✗. Как отмечалось выше (п. 1), стойкость редуцированной схемы существенно зависит от наличия операции `MixColumns`.

В четвёртом столбце указан объём материала, необходимый для проведения атаки. Под объёмом материала понимается количество пар открытых и соответствующих им шифрованных текстов, известных атакующему. Атаки на AES-128 используют один из трёх возможных типов необходимого материала: произвольные известные открытые тексты (ИО), подобранные открытые тексты (ПО) или подобранные шифрованные тексты (ПШ). Тип материала указан в пятом столбце.

В шестом столбце указывается емкостная сложность атак, измеряемая в блоках AES-128 (длина одного блока составляет 16 байтов). Отметим, что некоторые авторы атак указывают объём используемой памяти приближённо. Например, в [33] приводятся атаки, требующие памяти порядка одного блока AES-128. В данном обзоре такие оценки не уточняются и приводятся в соответствии с источником.

В седьмом столбце указана вычислительная сложность (или трудоёмкость) атак. Следуя общепринятой терминологии, трудоёмкость атаки на k раундов AES-128 ($k = 1, 2, \ldots, 10$) будем измерять в операциях зашифрования (или эквивалентно — расшифрования) одного 16-байтового блока с помощью k раундов AES-128. В редких случаях обращение в память (*memory access*) является основной элементарной операцией атаки. Для таких атак трудоёмкость измеряется в количестве операций доступа в память (ДП). Отметим, что некоторые атаки требуют проведения предварительных вычислений. Вычисления, которые необходимо произвести один раз, позволяют многократно атаковать шифр с меньшей трудоёмкостью. Например, трудоёмкость предварительного этапа атаки 68 составляет 2^{123}, а оперативного — 2^{113}. В сравнительной таблице трудоёмкость указана в худшем случае, в том числе с учётом предварительного этапа.

В восьмом столбце указан основной математический метод, используемый в атаке (или тип атаки). Типы атак, указанные в таблицах, являются условными. Как отме-

чалось выше, многие атаки совмещают несколько различных подходов. Кроме того, даже предлагаемые авторами классификации своих атак не всегда соответствуют распространённому пониманию тех или иных методов. Например, атаки 1, 6 и 17 отнесены их авторами к методу «встреча посередине», хотя они и не используют память. Тем не менее в таблицах указывается тип атаки в соответствии с источником.

В девятом столбце таблицы указана ссылка на работу, в которой предложена атака.

В некоторых работах указаны не все характеристики. Например, многие авторы зачастую не приводят оценок емкостных сложностей своих атак. Получение таких характеристик не всегда тривиально и может быть связано с детальным изучением отдельно взятых атак. В этих случаях в таблице стоит прочерк. Цветом выделены атаки, которые реализованы их авторами программно. В некоторых случаях исходные коды программ доступны в сети Интернет.

Атаки на редуцированный AES-128

№	Раунд	MC	Объём мат.	Тип мат.	Память	Трудоём.	Тип атаки	Работа
1	2	3	4	5	6	7	8	9
1	1	✓	1	ИО	1	2^{40}	Встр. посеред.	[25]
2	1	✓	1	ИО	2^{24}	2^{32}	Встр. посеред.	[25]
3	1	✓	2	ИО	1	2^{12}	Разностн.	[25]
4	1	✓	1	ИО	—	2^{48}	—	[6]
5	1	✓	1	ИО	2^{32}	2^{16}	—	[33]
6	2	✓	1	ИО	1	2^{80}	Встр. посеред.	[25]
7	2	✓	1	ИО	2^{49}	2^{64}	Встр. посеред.	[25]
8	2	✓	2	ИО	1	2^{48}	Разностн.	[25]
9	2	✓	2	ПО	1	2^{28}	Разностн.	[25]
10	2	✓	3	ИО	1	2^{32}	Разностн.	[25]
11	2	✗	2	ПО	—	2^{29}	Разностн.	[36]
12	2	✗	1	ИО	1	2^{56}	—	[33]
13	2	✗	2	ИО	2^{16}	2^{24}	—	[33]
14	2	✓	1	ИО	2^{48}	2^{64}	—	[33]
15	2	✓	2	ИО	2^{24}	2^{32}	Встр. посеред.	[33]
16	2	✓	2	ПО	2^{8}	2^{8}	—	[33]
17	3	✓	1	ИО	1	2^{120}	Встр. посеред.	[25]
18	3	✓	1	ИО	2^{49}	2^{104}	Встр. посеред.	[25]
19	3	✓	2	ПО	1	2^{32}	Разностн.	[25]
20	3	✓	9	ИО	2^{35}	2^{40}	Разн., Встр.	[25]
21	3	✗	1	ИО	2^{88}	2^{88}	—	[33]
22	3	✗	2	ИО	2^{80}	2^{80}	—	[33]
23	3	✗	2	ПО	2^{16}	2^{24}	—	[33]
24	3	✓	1	ИО	2^{72}	2^{96}	—	[33]
25	3	✓	2	ПО	2^{8}	2^{16}	—	[33]
26	3	✗, ✓	2	ПО	2^{8}	$2^{31,55}+2^{32}$ДП	Усеч. разност.	[4]
27	3	✗, ✓	3	ПО	1	$2^{11,2}$	Усеч. разност.	[4]
28	3	✗, ✓	3	ПО	2^{12}	$2^{5,1}+2^{10}$ДП	Усеч. разност.	[4]
29	4	✗	2^{9}	ПО	1	2^{9}	Квадрат	[7]
30	4	✓	2	ПО	1	2^{104}	Разн., Встр.	[25]
31	4	✓	5	ПО	2^{68}	2^{64}	Разн., Встр.	[25]
32	4	✓	10	ПО	2^{43}	2^{40}	Разн., Встр.	[25]
33	4	✗	12	ПО	—	2^{55}	Разностн.	[36]
34	4	✗	30	ПО	—	2^{54}	Разностн.	[36]
35	4	✗	2^{11}	ПО	—	2^{52}	Разностн.	[36]
36	4	✓	1	ИО	2^{80}	2^{120}	Встр. посеред.	[33]
37	4	✓	2	ПО	2^{80}	2^{80}	Встр. посеред.	[33]
38	4	✓	2^{2}	ПО	2^{24}	2^{32}	Встр. посеред.	[33]
39	4	✗	2^{9}	ПО	—	2^{8}	Квадрат	[16]

Окончание таблицы

№	Раунд	МС	Объём мат.	Тип мат.	Память	Трудоём.	Тип атаки	Работа
1	2	3	4	5	6	7	8	9
40	4	✗, ✓	2^3	ПО	2^{15}	2^{38}	Запрет. полит.	[19]
41	4	✗, ✓	2	ПО	1	2^{96}	Усеч. разност.	[4]
42	4	✗, ✓	3	ПО	1	$2^{74,7}$	Усеч. разност.	[4]
43	4	✗, ✓	3	ПО	2^{12}	$2^{64}+2^{76}$ДП	Усеч. разност.	[4]
44	4	✗, ✓	24	ПО	2^{17}	$2^{33,9}+2^{40,6}$ДП	Усеч. разност.	[4]
45	5	✗	2^{11}	ПО	1	2^{40}	Квадрат	[7]
46	5	✗	2^{32}	ПО	2^{32}	2^{40}	Квадрат	[7]
47	5	✗	2^{11}	ПО	—	2^{39}	Квадрат	[16]
48	5	✗	$2^{29,5}$	ПО	—	2^{31}	Запрет. разн.	[16]
49	5	✗	2^8	ПО	—	$2^{37,5}$	Квадрат	[36]
50	5	✗	2^8	ПО	—	2^{38}	Частич. сумм.	[22]
51	5	✗, ✓	15	ПО	2^{41}	2^{70}	Запрет. полит.	[19]
52	6	✗	$6 \cdot 2^{32}$	ПО	—	2^{44}	Частич. сумм.	[21]
53	6	✗	$2^{108,5}$	ИО	—	2^{120}	Разн., Встр.	[25]
54	6	✗	2^{32}	ПО	2^{32}	2^{72}	Квадрат	[7]
55	6	✗	2^{32}	ПО	—	2^{71}	Квадрат	[16]
56	6	✗	$2^{91,5}$	ПО	2^{89}	2^{122}	Запрет. разн.	[37]
57	6	—	$2^{114,5}$	ПО	—	2^{50}	Запрет. разн.	[38]
58	6	—	$2^{75,5}$	ПО	—	2^{104}	Запрет. разн.	[38]
59	6	✗	2^{32}	ПО	2^{40}	2^{42}	Частич. сумм.	[22]
60	6	✗	$2 \cdot 2^{32}$	ПО	—	—	Частич. сумм.	[39]
61	6	✗	2^8	ПО	$2^{106,17}$	$2^{106,17}$	Встр. посеред.	[34]
62	7	✗	2^{32}	ПО	2^{32}	$\approx 2^{128}$	Встр. (коллиз.)	[28]
63	7	✗	$2^{128}-2^{119}$	ПО	2^{64}	2^{120}	Частич. сумм.	[21]
64	7	✗	$2^{117,5}$	ПО	2^{105}	2^{123}	Запрет. разн.	[40]
65	7	✗	$2^{112,2}$	ПО	—	$2^{117,2}$ ДП	Запрет. разн.	[18]
66	7	—	$2^{115,5}$	ПО	2^{41}	2^{119}	Запрет. разн.	[38]
67	7	—	$2^{115,5}$	ПО	2^{105}	2^{119}	Запрет. разн.	[41]
68	7	—	2^{80}	ПО	2^{122}	2^{123}	Встр. посеред.	[30]
69	7	—	$2^{115,32}$	ПО	—	$2^{119,32}$	Запр. разн.	[42]
70	7	✗	2^{103+k}	ПО	2^{103+k}	2^{129-k}	Встр. (коллиз.)	[43]
71	7	—	$2^{106,2}$	ПО	$2^{90,2}$	$2^{107,1}+2^{117,2}$ДП	Запрет. разн.	[44]
72	7	✗	2^{105}	ПО	2^{90}	2^{99}	Встр. посеред.	[45]
73	7	✗	2^{99}	ПО	2^{96}	2^{99}	Встр. посеред.	[45]
74	7	—	2^{80}	ПО	2^{65}	2^{127}	Запрет. разн.	[46]
75	7	✗	2^{32}	ПО	$2^{126,47}$	$2^{126,47}$	Встр. посеред.	[34]
76	8	✗	$2^{126,33}$	ПШ	2^{102}	$2^{124,97}$	Биклик	[2]
77	8	✗	2^{127}	ПШ	2^{32}	$2^{125,64}$	Биклик	[2]
78	8	✗	2^{88}	ПШ	2^8	$2^{125,34}$	Биклик	[2]
79	10	✗	2^4	ПО	2^8	$2^{126,89}$	Биклик	[47]
80	10	✗	2^{88}	ПШ	2^8	$2^{126,18}$	Биклик	[2]
81	10	✗	2^{88}	ПШ	2^{64}	$2^{125,69}$	Биклик, Прос.	[24]
82	10	✗	2^{128}	ИО	2^8	$2^{125,56}$	Биклик	[26]
83	10	✗	2^{128}	ИО	2^{64}	$2^{125,35}$	Биклик, Прос.	[26]
84	10	✗	2^{64}	ПШ	2^8	$2^{126,16}$	Биклик	[26]
85	10	✗	2^{64}	ПШ	2^{64}	$2^{125,98}$	Биклик, Прос.	[26]
86	10	✗	2	ИО	2^8	$2^{126,67}$	Биклик	[26]
87	10	✗	2	ИО	2^{64}	$2^{126,59}$	Биклик, Прос.	[26]
88	10	✗	2^{24}	ПШ	2^9	$2^{126,5}$	Биклик	[48]

Численные характеристики атак приведены в соответствии с первоисточником, за некоторым исключением. Из работы [44] взяты оценки емкостной сложности атак 56, 63 и 66, а также все характеристики атаки 67. Из работы [26] взяты характеристики атак 81 и 79. В соответствии с [4] приводится информация о том, что трудоёмкость

атак 40 и 51 не зависит от наличия операции `MixColumns` на последнем раунде редуцированного шифра.

Особо подчеркнём важность обращения к первоисточникам при цитировании характеристик атак. Некоторые авторы, ссылаясь на более ранние атаки, указывают характеристики, отличные от приведённых в исходных работах. Примеры публикаций новых оценок характеристик более ранних атак можно найти в работах М. Танстолла [22, 36] и китайских учёных [38]. Как правило, комментариев к подобным оценкам не имеется. Можно предположить, что новые оценки получены в результате более тщательного анализа трудоёмкости.

Необходимо также отметить, что численные оценки характеристик атак являются субъективными и иногда имеют нестрогое обоснование. Зашифрование (расшифрование) одного блока AES-128 зачастую не является основной элементарной операцией атаки и пересчёт производится с определёнными допущениями. Например, в [28] приводится атака (см. атаку 62 в таблице) с опробованием всех 2^{128} вариантов ключа. По заявлению авторов, операция отбраковки одного варианта ключа требует меньше времени, чем одна операция зашифрования (расшифрования) AES-128. В соответствии с [38] данная трудоёмкость оценивается как $\approx 2^{128}$.

Другим примером неоднозначности характеристик атак на AES служит оценка вычислительной трудоёмкости атаки 81. В исходной работе [24] не приводится точной оценки трудоёмкости атаки. Однако в [26] авторы метода «Биклик» цитируют атаку 81 с оценкой трудоёмкости в $2^{125{,}69}$ операций шифрования, при этом отмечая, что по их подсчётам трудоёмкость составляет $2^{125{,}98}$.

5. Сравнение атак на AES-128 и атаки с практической трудоёмкостью

Тенденция развития методов анализа AES такова, что большинство авторов стремится атаковать большее число раундов с трудоёмкостью, меньшей тотального опробования. Реже криптографы сосредотачиваются на атаках практической трудоёмкости на малое число раундов [11]. В данном обзоре не рассматривается вопрос о возможном применении методов понижения стойкости большого числа раундов AES-128 для формулирования атаки на меньшее число раундов с практической трудоёмкостью.

Как предложено в [11], будем говорить о практической атаке на редуцированный AES, если трудоёмкость не превышает 2^{56} операций шифрования.

В модели с одной известной парой открытого и шифрованного текстов с практической трудоёмкостью удаётся атаковать два раунда AES-128 (атака 12), а с трудоёмкостью, близкой к практической, — два полных раунда AES-128 (атака 14). Использование двух пар открытого и шифрованного текстов позволяет атаковать два полных раунда уже с практической трудоёмкостью (атака 15).

Если рассматривать модель с произвольным числом пар известных открытых и шифрованных текстов, то можно атаковать с практической трудоёмкостью максимально три полных раунда AES-128 (атака 20). Для этого потребуется всего девять пар шифрованных и открытых текстов. Атака комбинирует разностный метод и метод «встреча посередине».

В модели подобранных открытых текстов максимальное число раундов AES-128, атакуемых с практической трудоёмкостью, равно шести. Атака опубликована в 2014 г. (см. атаку 60). Авторы верифицировали атаку с помощью программной реализации предлагаемого метода. С использованием шести персональных компьютеров (с четырёхъядерным процессором и 8-гигабайтной оперативной памятью каждый) секретный

ключ был найден за 12 дней. Исходные коды программы, реализующей атаку, имеются в свободном доступе в сети Интернет.

На семь раундов AES-128 неизвестно атак с трудоёмкостью меньшей чем 2^{99} операций шифрования.

Большинство атак на AES-128 основывается на нескольких идеях и свойствах шифра, описанных в том числе ещё в исходной работе 1998 г., представляющей алгоритм Rijndael. Наиболее сильные атаки практической трудоёмкости используют метод «Квадрат». Наиболее сильные атаки теоретического понижения стойкости большого числа раундов AES основаны на методах «встреча посередине» и «Биклик» и их комбинациях. С использованием метода запретных разностей, как правило, формулируются наименее сильные атаки.

Заключение

Список литературы, посвящённой анализу американского стандарта шифрования, насчитывает несколько десятков работ, в каждой из которых описывается не один вариант атаки на AES при различных дополнительных условиях. Цель данной работы — составление наиболее полного обзора опубликованных атак.

Приведены характеристики 88 атак на редуцированные варианты AES-128. В поле зрения не попали атаки по побочным каналам и атаки с ограничением на используемые ключи. Как правило, атаки на AES-128 допускают обобщения для AES-192 и AES-256. В рамках данного обзора не проводилось подробное табулирование атак на два последних варианты алгоритма.

Самыми сильными атаками, понижающими теоретическую стойкость, являются атаки типа «Биклик», применённые впервые к AES в 2011 г. С помощью данного метода удаётся построить атаку на десять раундов AES-128 (нередуцированный вариант) с трудоёмкостью $2^{126{,}67}$ операций шифрования и с незначительным использованием памяти в модели с двумя известными парами открытого и шифрованного текстов.

Максимальное количество раундов AES-128, которое удаётся атаковать с практической трудоёмкостью, равно шести (атака опубликована в 2014 г.). Такое количество раундов достигается с помощью метода частичных сумм, поэтому для атаки необходимо 2^{33} подобранных открытых текстов.

В модели с несколькими известными парами открытого и шифрованного текстов с практической трудоёмкостью можно атаковать три полных раунда AES-128. Атака основана на комбинации разностного метода и метода «встреча посередине» и требует девяти пар открытого и шифрованного текстов.

ЛИТЕРАТУРА

1. `http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf` — National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard. 2001.
2. *Bogdanov A., Khovratovich D., and Rechberger C.* Biclique cryptanalysis of the full AES // ASIACRYPT 2011. LNCS. 2011. V. 7073. P. 344–371.
3. *Gilbert H. and Peyrin T.* Super-sbox Cryptanalysis: Improved Attacks for AES-like Permutations. Cryptology ePrint Archive, Report 2009/531. 2009.
4. *Grassi L., Rechberger C., and Ronjom S.* Subspace Trail Cryptanalysis and its Applications to AES. Cryptology ePrint Archive, Report 2016/592. 2016.
5. *Daemen J. and Rijmen V.* The Design of Rijndael: AES — The Advanced Encryption Standard. Berlin: Springer, 2002. 238 p.

6. *Dunkelman O. and Keller N.* The effects of the omission of last round's mixcolumns on AES // Inform. Proc. Let. 2010. V. 110. No. 8–9. P. 304–308.
7. *Daemen J. and Rijmen V.* AES Proposal: Rijndael. 1998. `http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf`.
8. *Bouillaguet C., Derbez P., Dunkelman O., et al.* Low-data complexity attacks on AES // IEEE Trans. Inform. Theory. 2012. V. 58. No. 11. P. 7002–7017.
9. *Bulygin S. and Brickenstein M.* Obtaining and solving systems of equations in key variables only for the small variants of AES. Cryptology ePrint Archive, Report 2008/435. 2008.
10. *Van Tilborg H.* Encyclopedia of Cryptography and Security. Berlin: Springer, 2005. 684 p.
11. *Tunstall M.* Practical complexity differential cryptanalysis and fault analysis of AES // J. Cryptographic Eng. 2011. V. 1. No. 3. P. 219–230.
12. *Bogdanov A. and Pyshkin A.* Algebraic Side-Channel Collision Attacks on AES. Cryptology ePrint Archive, Report 2007/477. 2007.
13. *Osvik D. A., Shamir A., and Tromer E.* Cache Attacks and Countermeasures: the Case of AES. Cryptology ePrint Archive, Report 2005/271. 2005.
14. *Ali S. S., Mukhopadhyay D., and Tunstall M.* Differential Fault Analysis of AES: Towards Reaching its Limits. Cryptology ePrint Archive, Report 2012/446. 2012.
15. *Biryukov A., Dunkelman O., Keller N., et al.* Key Recovery Attacks of Practical Complexity on AES Variants with up to 10 Rounds. Cryptology ePrint Archive, Report 2009/374. 2009.
16. *Biham E. and Keller N.* Cryptanalysis of reduced variants of Rijndael // Proc. 3rd AES Conf. N. Y., 1999. P. 11–15.
17. *Knudsen L. R.* Truncated and higher order differentials // LNCS. 1995. V. 1008. P. 196–211.
18. *Lu J., Dunkelman O., Keller N., and Kim J.* New Impossible Differential Attacks on AES. Cryptology ePrint Archive, Report 2008/540. 2008.
19. *Tiessen T.* Polytopic cryptanalysis // Proc. 35th Ann. Intern. Conf. Advances in Cryptology — EUROCRYPT 2016. V. 9665. N. Y.: Springer, 2016. P. 214–239.
20. *Daemen J., Knudsen L., and Rijmen V.* The block cipher square // LNCS. 1997. V. 1267. P. 149–165.
21. *Ferguson N., Kelsey J., Lucks S., et al.* Improved cryptanalysis of Rijndael // LNCS. 2000. V. 1978. P. 213–230.
22. *Tunstall M.* Improved partial sums-based square attack on AES. Cryptology ePrint Archive, Report 2012/280. 2012.
23. *Leander G., Abdelraheem M. A., AlKhzaimi H., and Zenner E.* A cryptanalysis of PRINTcipher: The invariant subspace attack // CRYPTO 2011. LNCS. 2011. V. 6841. P. 206–221.
24. *Canteaut A., Naya-Plasencia M., and Vayssiere B.* Sieve-in-the-Middle: Improved MITM Attacks (full version). Cryptology ePrint Archive, Report 2013/324. 2013.
25. *Bouillaguet C., Derbez P., Dunkelman O., et al.* Low Data Complexity Attacks on AES. Cryptology ePrint Archive, Report 2010/633. 2010.
26. *Bogdanov A., Chang D., Ghosh M., and Sanadhya S. K.* Bicliques with Minimal Data and Time Complexity for AES (extended version). Cryptology ePrint Archive, Report 2014/932. 2014.
27. *Li L., Jia K., and Wang X.* Improved Meet-in-the-Middle Attacks on AES-192 and PRINCE. Cryptology ePrint Archive, Report 2013/573. 2013.
28. *Gilbert H. and Minier M.* A collision attack on the 7-rounds Rijndael // AES Candidate Conference. N. Y., 2000. P. 230–241.

29. *Demirci H. and Selcuk A.* A meet-in-the-middle attack on 8-round AES // FSE. LNCS. 2008. V. 5086. P. 116–126.
30. *Demirci H., Taskn I., Coban M., and Baysal A.* Improved meet-in-the-middle attacks on AES // INDOCRYPT 2009. LNCS. 2009. V. 5922. P. 144–156.
31. *Xiaoli D., Yupu H., Yongzhuang W., and Jie C.* A new method for meet-in-the-middle attacks on reduced AES // Wireless Communication Over Zigbee for Automotive Inclination Measurement. China Communications. 2011. V. 8. No. 2. P. 21–25.
32. *Wei Y., Lu J., and Hu Y.* Meet-in-the-Middle Attack on 8 Rounds of the AES Block Cipher under 192 Key Bits. Cryptology ePrint Archive, Report 2010/537. 2010.
33. *Bouillaguet C., Derbez P., and Fouque P.-A.* Automatic Search of Attacks on Round-Reduced AES and Applications. Cryptology ePrint Archive, Report 2012/069. 2012.
34. *Derbez P. and Fouque P.-A.* Exhausting Demirci-Selcuk Meet-in-the-Middle Attacks against Reduced-Round AES. Cryptology ePrint Archive, Report 2015/259. 2015.
35. *Biryukov A. and Nikolić I.* Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and others. Cryptology ePrint Archive, Report 2010/248. 2010.
36. *Tunstall M.* Practical Complexity Differential Cryptanalysis and Fault Analysis of AES. Cryptology ePrint Archive, Report 2011/453. 2011.
37. *Cheon J. H., Kim M., Kim K., et al.* Improved impossible differential cryptanalysis of Rijndael and Crypton // ICISC 2001. LCNS. 2002. V. 2288. P. 39–49.
38. *Zhang W., Wu W., and Feng D.* New results on impossible differential cryptanalysis of reduced AES // ICISC 2007. LCNS. 2007. V. 4817. P. 239–250.
39. *Alda F., Aragona R., Nicolodi L., and Sala M.* Implementation and Improvement of the Partial Sum Attack on 6-Round AES. Cryptology ePrint Archive, Report 2014/216. 2014.
40. *Bahrak B. and Aref M.* A novel impossible differential cryptanalysis of AES // Western European Workshop on Research in Cryptology. Bochum, 2007. P. 152-156.
41. *Bahrak B. and Aref M.* Impossible differential attack on seven-round AES-128 // IET Inform. Sec. 2008. V. 2. No. 2. P. 28–32.
42. *Yuan Z.* New Impossible Differential Attacks on AES. Cryptology ePrint Archive, Report 2010/093. 2010.
43. *Dunkelman O., Keller N., and Shamir A.* Improved Single-Key Attacks on 8-round AES. Cryptology ePrint Archive, Report 2010/322. 2010.
44. *Mala H., Dakhilalian M., Rijmen V., and Modarres-Hashemi M.* Improved impossible differential cryptanalysis of 7-round AES-128 // INDOCRYPT 2010. LNCS. 2010. V. 6498. P. 282–291.
45. *Derbez P., Fouque P.-A., and Jean J.* Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting. Cryptology ePrint Archive, Report 2012/477. 2012.
46. *Liu Y., Gu D., Liu Z., et al.* New improved impossible differential attack on reduced-round AES-128 // Lecture Notes Electr. Eng. 2012. V. 114. P. 453–461.
47. *Bogdanov A., Kavun E. B., Paar C., et al.* Better than brute-force optimized hardware architecture for efficient biclique attacks on AES-128 // SHARCS12 — Special-Purpose Hardware for Attacking Cryptographic Systems. Washington, 2012. P. 17–34.
48. *Chang D., Ghosh M., and Sanadhya S.* Biclique Cryptanalysis of Full Round AES with Reduced Data Complexity. IIIT Delhi. 2013. `https://repository.iiitd.edu.in/jspui/handle/123456789/99`.

REFERENCES

1. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf — National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard, 2001.
2. *Bogdanov A., Khovratovich D., and Rechberger C.* Biclique cryptanalysis of the full AES. ASIACRYPT 2011, LNCS, 2011, vol. 7073, pp. 344–371.
3. *Gilbert H. and Peyrin T.* Super-sbox Cryptanalysis: Improved Attacks for AES-like Permutations. Cryptology ePrint Archive, Report 2009/531, 2009.
4. *Grassi L., Rechberger C., and Ronjom S.* Subspace Trail Cryptanalysis and its Applications to AES. Cryptology ePrint Archive, Report 2016/592, 2016.
5. *Daemen J. and Rijmen V.* The Design of Rijndael: AES — The Advanced Encryption Standard. Berlin, Springer, 2002, 238 p.
6. *Dunkelman O. and Keller N.* The effects of the omission of last round's mixcolumns on AES. Inform. Proc. Let., 2010, vol. 110, no. 8–9, pp. 304–308.
7. *Daemen J. and Rijmen V.* AES Proposal: Rijndael. 1998. http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf.
8. *Bouillaguet C., Derbez P., Dunkelman O., et al.* Low-data complexity attacks on AES. IEEE Trans. Inform. Theory, 2012, vol. 58, no. 11, pp. 7002–7017.
9. *Bulygin S. and Brickenstein M.* Obtaining and solving systems of equations in key variables only for the small variants of AES. Cryptology ePrint Archive, Report 2008/435, 2008.
10. *Van Tilborg H.* Encyclopedia of Cryptography and Security. Berlin, Springer, 2005, 684 p.
11. *Tunstall M.* Practical complexity differential cryptanalysis and fault analysis of AES. J. Cryptographic Eng., 2011, vol. 1, no. 3, pp. 219–230.
12. *Bogdanov A. and Pyshkin A.* Algebraic Side-Channel Collision Attacks on AES. Cryptology ePrint Archive, Report 2007/477, 2007.
13. *Osvik D. A., Shamir A., and Tromer E.* Cache Attacks and Countermeasures: the Case of AES. Cryptology ePrint Archive, Report 2005/271, 2005.
14. *Ali S. S., Mukhopadhyay D., and Tunstall M.* Differential Fault Analysis of AES: Towards Reaching its Limits. Cryptology ePrint Archive, Report 2012/446, 2012.
15. *Biryukov A., Dunkelman O., Keller N., et al.* Key Recovery Attacks of Practical Complexity on AES Variants with up to 10 Rounds. Cryptology ePrint Archive, Report 2009/374, 2009.
16. *Biham E. and Keller N.* Cryptanalysis of reduced variants of Rijndael. Proc. 3rd AES Conf., N. Y., 1999, pp. 11–15.
17. *Knudsen L. R.* Truncated and higher order differentials. LNCS, 1995, vol. 1008, pp. 196–211.
18. *Lu J., Dunkelman O., Keller N., and Kim J.* New Impossible Differential Attacks on AES. Cryptology ePrint Archive, Report 2008/540, 2008.
19. *Tiessen T.* Polytopic cryptanalysis. Proc. 35th Ann. Intern. Conf. Advances in Cryptology — EUROCRYPT 2016, vol. 9665, N. Y., Springer, 2016, pp. 214–239.
20. *Daemen J., Knudsen L., and Rijmen V.* The block cipher square. LNCS, 1997, vol. 1267, pp. 149–165.
21. *Ferguson N., Kelsey J., Lucks S., et al.* Improved cryptanalysis of Rijndael. LNCS, 2000, vol. 1978, pp. 213–230.
22. *Tunstall M.* Improved partial sums-based square attack on AES. Cryptology ePrint Archive, Report 2012/280, 2012.
23. *Leander G., Abdelraheem M. A., AlKhzaimi H., and Zenner E.* A cryptanalysis of PRINTcipher: The invariant subspace attack. CRYPTO 2011, LNCS, 2011, vol. 6841, pp. 206–221.

24. *Canteaut A., Naya-Plasencia M., and Vayssiere B.* Sieve-in-the-Middle: Improved MITM Attacks (full version). Cryptology ePrint Archive, Report 2013/324, 2013.
25. *Bouillaguet C., Derbez P., Dunkelman O., et al.* Low Data Complexity Attacks on AES. Cryptology ePrint Archive, Report 2010/633, 2010.
26. *Bogdanov A., Chang D., Ghosh M., and Sanadhya S. K.* Bicliques with Minimal Data and Time Complexity for AES (extended version). Cryptology ePrint Archive, Report 2014/932, 2014.
27. *Li L., Jia K., and Wang X.* Improved Meet-in-the-Middle Attacks on AES-192 and PRINCE. Cryptology ePrint Archive, Report 2013/573, 2013.
28. *Gilbert H. and Minier M.* A collision attack on the 7-rounds Rijndael. AES Candidate Conference, N. Y., 2000, pp. 230–241.
29. *Demirci H. and Selcuk A.* A meet-in-the-middle attack on 8-round AES. FSE, LNCS, 2008, vol. 5086, pp. 116–126.
30. *Demirci H., Taskn I., Coban M., and Baysal A.* Improved meet-in-the-middle attacks on AES. INDOCRYPT 2009, LNCS, 2009, vol. 5922, pp. 144–156.
31. *Xiaoli D., Yupu H., Yongzhuang W., and Jie C.* A new method for meet-in-the-middle attacks on reduced AES. Wireless Communication Over Zigbee for Automotive Inclination Measurement. China Communications, 2011, vol. 8, no. 2, pp. 21–25.
32. *Wei Y., Lu J., and Hu Y.* Meet-in-the-Middle Attack on 8 Rounds of the AES Block Cipher under 192 Key Bits. Cryptology ePrint Archive, Report 2010/537, 2010.
33. *Bouillaguet C., Derbez P., and Fouque P.-A.* Automatic Search of Attacks on Round-Reduced AES and Applications. Cryptology ePrint Archive, Report 2012/069, 2012.
34. *Derbez P. and Fouque P.-A.* Exhausting Demirci-Selcuk Meet-in-the-Middle Attacks against Reduced-Round AES. Cryptology ePrint Archive, Report 2015/259, 2015.
35. *Biryukov A. and Nikolić I.* Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad and others. Cryptology ePrint Archive, Report 2010/248, 2010.
36. *Tunstall M.* Practical Complexity Differential Cryptanalysis and Fault Analysis of AES. Cryptology ePrint Archive, Report 2011/453, 2011.
37. *Cheon J. H., Kim M., Kim K., et al.* Improved impossible differential cryptanalysis of Rijndael and Crypton. ICISC 2001, LCNS, 2002, vol. 2288, pp. 39–49.
38. *Zhang W., Wu W., and Feng D.* New results on impossible differential cryptanalysis of reduced AES. ICISC 2007, LCNS, 2007, vol. 4817, pp. 239–250.
39. *Alda F., Aragona R., Nicolodi L., and Sala M.* Implementation and Improvement of the Partial Sum Attack on 6-Round AES. Cryptology ePrint Archive, Report 2014/216, 2014.
40. *Bahrak B. and Aref M.* A novel impossible differential cryptanalysis of AES. Western European Workshop on Research in Cryptology, Bochum, 2007, pp. 152-156.
41. *Bahrak B. and Aref M.* Impossible differential attack on seven-round AES-128. IET Inform. Sec., 2008, vol. 2, no. 2, pp. 28–32.
42. *Yuan Z.* New Impossible Differential Attacks on AES. Cryptology ePrint Archive, Report 2010/093, 2010.
43. *Dunkelman O., Keller N., and Shamir A.* Improved Single-Key Attacks on 8-round AES. Cryptology ePrint Archive, Report 2010/322, 2010.
44. *Mala H., Dakhilalian M., Rijmen V., and Modarres-Hashemi M.* Improved impossible differential cryptanalysis of 7-round AES-128. INDOCRYPT 2010, LNCS, 2010, vol. 6498, pp. 282–291.
45. *Derbez P., Fouque P.-A., and Jean J.* Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting. Cryptology ePrint Archive, Report 2012/477, 2012.

46. *Liu Y., Gu D., Liu Z., et al.* New improved impossible differential attack on reduced-round AES-128. Lecture Notes Electr. Eng., 2012, vol. 114, pp. 453–461.
47. *Bogdanov A., Kavun E. B., Paar C., et al.* Better than brute-force optimized hardware architecture for efficient biclique attacks on AES-128. SHARCS12 — Special-Purpose Hardware for Attacking Cryptographic Systems, Washington, 2012, pp. 17–34.
48. *Chang D., Ghosh M., and Sanadhya S.* Biclique Cryptanalysis of Full Round AES with Reduced Data Complexity. IIIT Delhi, 2013. `https://repository.iiitd.edu.in/jspui/handle/123456789/99`.