УДК 681.3.06:006.354

ОСНОВНЫЕ ПРИНЦИПЫ ПРОЕКТИРОВАНИЯ, ОЦЕНКА СТОЙКОСТИ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ В УКРАИНЕ АЛГОРИТМА ШИФРОВАНИЯ AES

Геннадий Гулак*, Иван Горбенко, Роман Олейников, Александр Шумов, Юрий Горбенко

АО «Институт Информационных Технологий»

**ДСТСЗИ СБ Украины*

Анотація: **Представлені основні принципи проектування алгоритму шифрування AES, оцінка їх обгрунтованості та прозорості. Зроблений огляд найбільш ефективних методів криптоаналізу FIPS-197. Розглянуті проблемні питання безпеки, котрі у перспективі можуть бути використані для реалізації ефективної аналітичної атаки на шифр. Наведені дані про продуктивність програмних і апаратних реалізацій AES.**

Summary: **Designing principles of AES, their validity and clearness are given. The review of the most effective cryptanalytical attacks of Rijndael is given. Potential weaknesses in security of FIPS-197 leading to possible implementation of effective analytical attacks on the cipher in the future are considered. Performance of software and hardware implementation of FIPS-197 is given.**

Ключові слова: **FIPS-197, AES, Rijndael, блоковий симетричний алгоритм шифрування, криптоаналіз, програмна реалізація, апаратна реалізація.**

Введение

В 2000 году завершен международный проект по созданию алгоритма шифрования AES (Advanced Encryption Standard). В результате интенсивной совместной работы ведущих криптологов мира были глубоко проанализированы и исследованы свойства 15 алгоритмов-кандидатов на стандарт симметричного блочного шифра XXI века. При выполнении проекта создана мощная методологическая и методическая база разработки и анализа симметричных блочных алгоритмов, позволившая выбрать из претендентов симметричный блочный шифр Rijndael. После окончания проекта алгоритм Rijndael исследовался специальными подразделениями Агентства национальной безопасности США на соответствие заданному уровню стойкости, возможностям и условиям применения для защиты несекретной информации в государственных и коммерческих структурах США. Таким образом, для замены алгоритма DES и Triple DES (FIPS-46-3) принят новый алгоритм симметричного блочного шифрования, который официально вступил в действие в качестве федерального стандарта США – AES (FIPS-197) [1].

Кроме того, в 2000-м году был начат проект NESSIE (New European Schemes for Signatures, Integrity and Encryption), целью которого является создание нескольких криптографических примитивов, среди которых есть и симметричный блочный шифр. По сути, к настоящему времени проект уже закончен, и приняты предварительные решения о том, что среди блочных алгоритмов лучшими являются Rijndael, Camellia и Shacal-2. Они, очевидно, и будут рекомендованы в качестве стандартов Европейского Союза.

В настоящее время в Украине официально рекомендован к применению симметричный блочный алгоритм шифрования ГОСТ 28147-89, который, по нашему мнению и критериям стойкости проекта NESSIE обеспечивает самый низкий (из допустимых) уровень безопасности – нормальный унаследованный. Поэтому весьма важной является задача оценки и выбора для применения в Украине одного из симметричных блочных шифров, прошедших глубокие исследования в процессе выполнения проектов AES и NESSIE. Целью настоящей статьи является обобщение результатов, полученных в ходе выполнения проектов AES и NESSIE, обоснование и формулирование рекомендаций для использования в Украине федерального стандарта США FIPS-197.

I Основные принципы проектирования алгоритма FIPS-197

Современные симметричные блочные алгоритмы шифрования имеют широкую сферу применения, включающую, кроме традиционного шифрования, построение кодов аутентификации сообщений, хэш-функций, протоколов аутентификации и т. д. Реализация алгоритма может выполняться аппаратно или программно, защита информации может обеспечиваться как в локальных системах, так и в телекоммуникационных сетях. В связи с этим к используемым и проектируемым блочным шифрам, в т. ч. FIPS-197 [1, 2] предъявляются жёсткие требования, среди которых можно выделить следующие [3 – 5].

1. Простое криптографическое ядро с прозрачными принципами его проектирования.

2. Стойкость, включающая в себя использование стойкого и проверенного криптографического ядра, соответствующей процедуры выработки подключей, отсутствие слабых ключей и лазеек; стойкость к известным методам криптоанализа, включая дифференциальный и линейный криптоанализ, временную атаку и т. п., – отсутствие аналитических атак, более эффективных, чем силовые атаки.
3. Простота реализации, подразумевающая возможность эффективного использования шифра на различных процессорах (от 8-битных до 64-битных), под разными операционными системами, возможность построения специализированных аппаратных средств, реализующих алгоритм.
4. Гибкость использования: возможность разработки на базе шифра функций хэширования, генераторов псевдослучайных чисел, кодов аутентификации сообщений и поточных шифров.
5. Высокая производительность, позволяющая реализовать преобразование с минимальным потреблением вычислительных ресурсов процессора.
6. Применимость при реализации на смарт-картах с обеспечением приемлемой производительности.
7. Приемлемая стоимость реализации.
8. Отсутствие патентных ограничений, что юридически позволяет разработчикам свободно использовать алгоритм в любых приложениях.

При проектировании алгоритма Rijndael разработчики использовали максимально прозрачные правила построения и представили доказательства стойкости к нескольким видам криптоанализа, которые могут быть применимы к шифру. Алгоритм имеет простую структуру, что позволяет достичь высокой производительности и выполнить эффективную реализацию на различных платформах, имеющую достаточно низкую стоимость. Среди всех кандидатов AES и NESSIE алгоритм Rijndael является одним из наиболее производительных и простых в реализации.

Шифр не имеет патентных ограничений и может свободно использоваться разработчиками в различных приложениях. К нынешнему моменту в открытых публикациях не описан ни один из методов, который позволил бы выполнить криптоанализ со сложностью, менее чем сложность силовой атаки на шифр.

В настоящее время алгоритм Rijndael соответствует всем вышеперечисленным требованиям. По результатам оценки конкретных показателей безопасности, производительности и простоты реализации Rijndael стал финалистом конкурсов AES и NESSIE, а в дальнейшем был принят в качестве федерального стандарта США (FIPS-197)

Алгоритм Rijndael построен на основе модифицированной SPN-структуры (Substitution-Permutation Network), и является шифром, использующим подстановку и линейное преобразование (substitution-linear transformation network) с 10, 12 или 14 циклами шифрования, в зависимости от длины ключа [3]. Алгоритм является байт-ориентированным и построен на основе предыдущей разработки авторов – шифре Square. Основное нелинейное преобразование – подстановка (S-box) имеет математическую структуру и может быть представлена как вычисление обратного элемента в поле $GF(2^8)$ и последующее аффинное преобразование. Подключи вводятся с использованием операции сложения по модулю 2 (XOR, EXOR). Рассеивание и распространение достигается за счёт байтовой перестановки (сдвига строк) и МДР-преобразования, гарантирующего максимальное расстояние Хэмминга между входными и выходными данными. Используемые преобразования являются достаточно известными и обладают хорошими криптографическими свойствами. Процедура выработки подключей имеет простую структуру, что обуславливает значительную неравномерность размножения ошибок в подключах, зависящую от номера бита в ключе шифрования [7]. Тем не менее, предложения некоторых исследователей изменить эту процедуру привели к ослаблению модифицированного варианта шифра.

В основе проектирования алгоритма лежит так называемая стратегия wide-trail («широкий след»), подразумевающая максимальное количество ветвей активизации и, соответственно, низкую вероятность нахождения верной пары характеристики в дифференциальном криптоанализе и выполнения аппроксимации в линейном криптоанализе.

Для устранения возможности появления путей активизации с низким числом ветвлений авторами шифра предлагаются следующие ограничения [8].

1. Осуществлять выбор подстановок (S-блоков) с минимальными дифференциальными и корреляционными значениями.
2. Выбирать цикловое преобразование таким образом, чтобы препятствовать возможности построения путей активизации с низким числом ветвлений.

Разработчики алгоритма подчёркивают дополнительное преимущество использования стратегии wide-trail за счёт использования эффективного циклового преобразования можно отказаться от применения подстановок большой размерности, что значительно сэкономит ресурсы системы (требования к объёму памяти) и позволит достичь хорошего распространения на нескольких циклах. При использовании этой стратегии в AES выполнено чередование линейного отображения и подстановки, что позволило достичь

высокой степени рассеивания в пределах одной подстановки и распространения в цикловой функции [8].

При выборе подстановки (S-блока) авторы руководствовались следующими критериями [2]:

- обратимость (биективность);
- минимизация наибольшего значения в таблице линейной аппроксимации подстановки;
- минимизация наибольшего значения в таблице распределения разностей;
- сложность алгебраического представления в поле $GF(2^8)$;
- простота описания.

В соответствии с рекомендациями, изложенными в [9], авторы выбрали мультипликативное обращение в поле $GF(2^8)$. Для предотвращения чрезвычайно простого алгебраического описания было добавлено аффинное преобразование, исключающее появление «фиксированных точек» $\left(\left\{x \in GF\left(2^8\right) \middle| S(x) = x\right\} = \varnothing\right)$ и «инвертированных фиксированных точек» $\left(\left\{x \in GF\left(2^8\right) \middle| S(x) = \bar{x}\right\} = \varnothing\right)$. Отмечается, что кроме варианта, предложенного авторами, существуют другие подстановки, обладающие необходимыми свойствами. Кроме того, благодаря структуре цикловой функции, шифр будет стойким к дифференциальному и линейному криптоанализу с большинством случайных подстановок, не удовлетворяющим перечисленным критериям.

Распространение в ходе шифрования является важным свойством, обуславливающим стойкость алгоритма, и обеспечивается преобразованием MixColumn. При его выборе авторы шифра руководствовались следующими критериями [2]:

- обратимость;
- линейность в GF(2);
- соответствующая степень распространения;
- возможность быстрой реализации на 8-битовых процессорах;
- симметрия;
- простота описания.

В соответствии с этими критериями авторами было выбрано умножение на полином 4-й степени в поле $GF(2^8)$.

Байтовая перестановка ShiftRow используется для распространения изменений одной колонки на весь блок и обеспечения защиты от дополнительных криптоаналитических атак. При выборе байтовой перестановки применялись следующие критерии [2]:

- все сдвиги строк являются различными, причём один из них выполняет тривиальное отображение (нулевой сдвиг);
- должна быть обеспечена защита от атаки усечённых дифференциалов;
- должна быть обеспечена защита от Square-атаки;
- преобразование должно быть максимально простым.

Из возможных вариантов был выбран наиболее простой.

Процедура разворачивания подключей, кроме обычных функций, дополнительно необходима для устранения симметрии внутри цикловой функции и однотипности разных циклов преобразования. При выборе процедуры использовались следующие критерии [2]:

- обратимость преобразования;
- высокая производительность на разных процессорах;
- наличие специальных констант для разных циклов для устранения однотипности циклов шифрования;
- распространение изменений ключа шифрования в изменения подключей;
- знание нескольких битов ключа шифрования или подключа не должно давать возможность вычислить остальные биты;
- нелинейность для предотвращения определения разности подключей по разности ключа шифрования;
- простота описания.

Разработанная процедура выработки подключей имеет низкую сложность и, соответственно, высокую производительность. Однако, благодаря простоте, реализация критерия распространения изменений ключа шифрования имеет недостаточно хорошие свойства [7], что впоследствии позволило реализовать атаку на 9 циклов (из 14) AES-256, основанную на связанных подключах [10]. Тем не менее, это свойство не удалось использовать в полном варианте шифра при любой длине ключа (128, 192 и 256 битов).

Кроме того, авторы алгоритма представили расчёт сложности [2] и математическое доказательство

стойкости шифра к дифференциальному и линейному криптоанализу [11].

В целом, при проектировании авторы старались следовать следующим критериям [12]:

- симметрия циклового преобразования и однотипность разных циклов;
- ортогональность компонентов шифра;
- отсутствие арифметических операций (по модулю, превышающему 2).

Симметрия преобразований позволяет выполнить эффективную реализацию алгоритма на процессорах с параллельной архитектурой (SIMD-инструкции, Single Instruction for Multiple Data), уменьшить объём кода за счёт использования вызовов одной функции и сократить объём необходимой памяти (т. к. используется только одна подстановка «байт-в-байт»).

Впоследствии, для того, чтобы симметрия циклового преобразования и однотипность разных циклов (первый критерий) не привела к уязвимости шифра, был сформулирован дополнительный критерий для процедуры выработки подключей.

Ортогональность компонентов позволяет значительно увеличить стойкость алгоритма за счёт усложнения алгебраического описания преобразований в целом.

Отсутствие арифметических операций позволяет значительно упростить аппаратную реализацию шифра в виде ПЛИС или заказной ИМС.

Авторы приводят следующие аргументы для принятия алгоритма Rijndael в качестве стандарта AES [12]:

- стойкость: Rijndael имеет высокий уровень стойкости, соответствующий остальным кандидатам-финалистам;
- эффективность: реализации Rijndael имеют значительное преимущество в производительности по сравнению с реализациями других алгоритмов;
- прозрачные принципы проектирования и простота, что позволяет убедиться в отсутствии закладок, выполнить простую и быстродействующую аппаратную и программную реализацию на множестве платформ и т. п.
- расширяемость: Rijndael может быть легко адаптирован к другим длинам ключей и блоков.

Исходя из представленных авторами алгоритма данных и результатов последующих исследований независимых специалистов, можно сделать вывод о том, что при проектировании шифра использовалась хорошо исследованная в криптографии математическая база. В отчётах, представленных вместе с алгоритмом, достаточно обоснованно и прозрачно излагаются принципы проектирования и критерии, по которым проводился выбор того или иного решения. Опираясь на интенсивные исследования шифра в течение последних пяти лет, можно ожидать, что заявление об отсутствии в шифре скрытых лазеек соответствует действительности.

Таким образом, опираясь на вышеизложенное, можно утверждать, что алгоритм Rijndael имеет должный уровень математического обоснования, принципы его проектирования достаточно прозрачны, и полностью опубликованы авторами шифра.

II Криптоанализ алгоритма шифрования FIPS-197

В настоящее время в открытых публикациях описано большое количество криптоаналитических атак против симметричных блочных алгоритмов шифрования. Как наиболее универсальные, следует выделить дифференциальный [13] и линейный криптоанализ [14]. Кроме того, на основе дифференциального криптоанализа разработана атака с использованием усечённых [15] и невыполнимых [16] дифференциалов. Для любого итеративного шифра, в т. ч. Rijndael, потенциально возможна атака на основе связанных ключей [17] и на основе коллизий байт-ориентированных функций в составе алгоритма [18]. Поскольку при построении Rijndael за основу был взят блочный шифр Square, возможно применение Square-атаки [19] вида интегрального криптоанализа [20]. Из перечисленных атак линейный криптоанализ относится к атакам на основе известных открытых сообщений, все остальные методы – к атакам на основе выбранных открытых сообщений.

Стойкость шифра должна быть тщательно проверена по отношению ко всем известным методам, и дополнительно необходимо провести поиск возможных уязвимостей, приводящих к потенциально эффективным аналитическим атакам.

При выполнении дифференциального криптоанализа производится исследование прохождения разностей шифруемых блоков через циклы алгоритма. Алгоритм уязвим к этому виду криптонападения в случае, если после определённого количества циклов шифрования (как правило, $N-3$, где N – количество циклов во всём алгоритме) вероятность появления заданной разности на выходе (выполнения дифференциальной характеристики) превышает значение $2^{-(n-1)}$, где n – размер шифруемого блока (в битах). Исключение

составляет бумеранг-атака, эффективная при существовании характеристик для $\frac{N}{2}$ циклов, но эта атака неприменима к AES [21].

При проектировании Rijndael была учтена возможность применения дифференциального криптоанализа. Более того, используемая стратегия wide-trail гарантирует стойкость шифра к этой атаке. По оценкам разработчиков алгоритма [2], максимальная вероятность 4-цикловой характеристики равна 2^{-150}, а 8-цикловой – 2^{-300}. Учитывая, что размер блока AES составляет $n = 128$ битов, а минимальное количество циклов шифрования равно 10, можно утверждать, что алгоритм является стойким к дифференциальному криптоанализу, и, более того, в шифре заложен большой запас стойкости по отношению к таким атакам.

Позже была выполнена более точная оценка стойкости кандидатов AES по отношению к дифференциальному криптоанализу, атаке с использованием усечённых и невыполнимых дифференциалов [22, 23] и подтверждена стойкость Rijndael к этим видам анализа.

Линейный криптоанализ применим к шифрам, в которых существует корреляция между блоками открытого и зашифрованного текста. Криптоаналитик, находя сумму некоторых битов открытого и зашифрованного текстов, получает сумму битов использованных цикловых подключей. Линейный криптоанализ, предложенный в [16], неприменим к шифрам, использующим операцию сложения по модулю $m > 2$ [24]. В алгоритме Rijndael используется только операция сложения по модулю $m = 2$, поэтому шифр (по крайней мере, несколько его циклов) потенциально уязвим для этой атаки.

В связи с этим при проектировании алгоритма разработчики учли возможность применения линейного криптоанализа. Использованная стратегия wide-trail гарантирует отсутствие линейных аппроксимаций на 4 цикла с вероятностью, превышающей 2^{-75}, и на 8 циклов, с вероятностью, превышающей 2^{-150}. Этого достаточно, чтобы предотвратить атаку на весь шифр, и, как и в случае с дифференциальным криптоанализом, в алгоритме заложен большой запас стойкости по отношению к этой атаке. Это результат подтверждён исследованиями, выполненными независимыми специалистами [25].

Таким образом, линейный криптоанализ не может быть использован против полного варианта алгоритма шифрования AES.

Атака с использованием усечённых дифференциалов может быть применена к шифру, если возможно объединение достаточно большого количества дифференциальных характеристик с определёнными входными и выходными разностями. В этом случае итоговая вероятность того, что выбранная разность останется в пределах кластера, может быть вычислена независимо от вероятностей отдельных характеристик [15, 2]. Шифры, выполняющие байт-ориентированные преобразования, потенциально более уязвимы к таким атакам, поэтому при построении алгоритма Rijndael была учтена возможность использования усечённых дифференциалов. Исследования авторов шифра [2] и дальнейшие уточнения независимых специалистов [22] показали, что атака может быть эффективна для 5 циклов шифрования и менее.

Поскольку атака была учтена при проектировании, алгоритм FIPS-197 является защищённым и от этого вида криптонападения.

Анализ с применением невыполнимых дифференциалов предполагает выбор входных и выходных разностей специальным образом, не допускающем существование верной пары характеристик для определённого множества ключей шифрования. В случае же появления верной пары при шифровании эти ключи исключаются из множества возможных, что сокращает множество потенциальных вариантов.

Авторы алгоритма не проводили исследования стойкости к анализу с применением невыполнимых дифференциалов. Дальнейшие исследования, использующие байт-ориентированную структуру шифра, показали, что такая атака может быть применена для 5-циклового [26] и 6-циклового [16] вариантов алгоритма.

Соответственно, 7 циклов шифрования и более, включая полный вариант алгоритма Rijndael, являются защищёнными от этой атаки.

Square-атака (интегральный криптоанализ) является одним из наиболее эффективных методов для алгоритма Rijndael. Атака применима к байт-ориентированным шифрам и впервые была применена для алгоритма Square [21]. Согласно исследованиям авторов шифра, базовый вариант Square-атаки может быть использован против 4 циклов алгоритма. Использование предположений о значении некоторых байтов цикловых подключей позволяет увеличить число атакуемых циклов до 6.

Более поздние исследования позволили использовать незначительную уязвимость в процедуре выработки подключей и разработать эффективную Square-атаку для 7 и 8 циклов шифрования [10, 27].

Полный вариант алгоритма шифрования AES при всех длинах ключей (128, 192 и 256 битов) остаётся неуязвимым для Square-атаки.

При выполнении атаки на основе связанных подключей при шифровании используются неизвестные

ключи с заданной криптоаналитиком зависимостью. Атака может быть разновидностью дифференциального криптоанализа или использовать особенности процедуры разворачивания подключей, после чего криптоаналитику становятся доступными промежуточные значения при шифровании (дальнейшее развитие это получило в слайд-атаке [29]).

По мнению авторов шифра [2], процедура разворачивания подключей обладает высокой степенью распространения и рассеивания, что делает атаку связанных ключей невероятной. Однако исследования показали значительную неравномерность размножения ошибок в подключах [7]. В дальнейшем этот факт был использован для реализации атаки связанных ключей на 9 циклов шифрования алгоритма Rijndael [10].

Тем не менее, достаточное количество циклов шифрования обеспечивают стойкость шифра и к этому виду криптонападения.

Атака на основе коллизий байт-ориентированных функций Rijndael [18] является специфичной, разработанной и в настоящее время известной исключительно для алгоритма Rijndael. В этой атаке используется факт, что существует отличие между 4 циклами шифрования AES и случайной перестановкой $\pi^R : \{0,1\}^{128} \to \{0,1\}^{128}$, что даёт возможность реализовать эффективную атаку на 7 циклов алгоритма. Данная атака, в отличие от предшествующих, не является статистической, и основана на использовании так называемого парадокса дней рождения. Успешное завершение гарантировано после выполнения сравнительно небольшого количества шифрований (примерно 2^{32}).

Полный вариант шифра является неуязвимым для криптоанализа на основе коллизий.

Для множества известных симметричных алгоритмов шифрования существуют так называемые слабые ключи, при которых некоторые криптографические свойства не выполняются. В частности, такие ключи существуют для IDEA [29], DES [30], ГОСТ 28147-89 и других алгоритмов. Как правило, количество таких ключей незначительно, вероятность их появления при генерации ничтожна, и дополнительно можно реализовать специальный фильтр для блокирования таких ключей шифрования. Однако при использовании алгоритма в составе хэш-функции, генератора псевдослучайных последовательностей, протокола аутентификации и т. п. контроль над ключом шифрования не всегда возможен. В этом случае возможно появление значительной уязвимости криптографического примитива, созданного на базе шифра.

К настоящему моменту таких ключей для алгоритма шифрования Rijndael не обнаружено. Более того, можно предположить, что благодаря введению в процедуру выработки подключей элементов, реализующих нелинейное преобразование, такие ключи вообще не существуют.

Единственным классом атак, который может быть эффективно использован злоумышленником против любого криптографического алгоритма с секретным ключом, является класс атак на реализацию (Side-Channel Attacks). В этом случае злоумышленник имеет доступ к аппаратной реализации шифратора, что позволяет ему управлять входом шифратора, производить измерения времени выполнения зашифрования/расшифрования, анализ энергопотребления, вносить сбои в работу аппаратного устройства/процессора и т. п. На основании побочной информации восстанавливается ключ шифрования.

Математическими методами или структурой алгоритма предотвратить такие атаки невозможно, и для них потенциально уязвимы все финалисты AES и NESSIE, ГОСТ 28147-89, DES, 3DES и другие алгоритмы.

Со времени представления алгоритма Rijndael как кандидата AES ведущими специалистами в области криптографических исследований было опубликовано более 20 работ, посвящённых изучению стойкости шифра. Часть результатов исследований авторов алгоритма, в частности, посвящённых дифференциальному и линейному криптоанализу, а также слабым ключам, была подтверждена в ходе независимых исследований. Ряд других криптоаналитических методов, в частности, Square-атака, были улучшены, что позволило реализовать атаку для большего числа циклов шифрования. В процедуре выработки подключей шифра была обнаружена незначительная уязвимость, что позволило реализовать атаку, которая, по заявлениям авторов, невозможна для шифра. При изучении свойств и особенностей построения Rijndael был разработан новый метод криптоанализа, использующий коллизии байт-ориентированных внутренних функций алгоритма.

Перечень методов криптоанализа, успешно применённых для алгоритма Rijndael [5] с уменьшенным количеством циклов, сложность проведения атаки (необходимое количество шифрований), а также требуемый объём данных приведен в табл. 1.

Как следует из табл. 1, для AES-128 был выполнен успешный криптоанализ 6 и 7 циклов шифрования из 10, причём для 7 циклов Square-атаки необходимый объём данных составляет всё множество открытых текстов. Минимальная сложность атаки 7 циклов равна 2^{120} операций шифрования.

Для AES-192 успешно были атакованы 7 циклов шифрования из 12. Минимальная сложность составила 2^{140} операций шифрования при необходимости 2^{32} выбранных пар открытого и зашифрованного текста.

При исследовании AES-256 были найдены атаки на 7, 8 и 9 циклов из 14. Сложность криптоанализа 7 циклов равна 2^{140} при необходимости 2^{32} выбранных пар открытого и зашифрованного текста. Атака на

9 циклов возможна только при наличии фиксированной зависимости между неизвестными ключами шифрования и требует практически недостижимого множества открытых текстов.

Таблица 1 – Сложность различных методов криптоанализа AES

Название атаки	Количество циклов	Сложность	Объём данных
Невыполнимые дифференциалы	5	2^{31}	$2^{29,5}$
Усечённые дифференциалы	7	2^{120}	2^{119}-2^{128}
Square (128-битовый ключ)	6	2^{44}	2^{32}
Square (128-битовый ключ)	7	2^{120}	2^{128}
Square (192-битовый ключ)	7	2^{155}	2^{32}
Square (256-битовый ключ)	8	2^{172}	2^{119}-2^{128}
Коллизии (128-битовый ключ)	7	2^{128}	2^{32}
Коллизии (192, 256-битовый ключ)	7	2^{140}	2^{32}
Связанные ключи (256-битовый ключ)	9	2^{224}	2^{77}

Таким образом, после 5 лет интенсивных исследований до сих пор в открытых источниках нет ни одной атаки, которая может быть эффективной для полноциклового варианта шифра, а по опубликованным атакам существует запас стойкости от 3 до 5 циклов. Кроме того, наличие прозрачных критериев и правил проектирования, сформулированных разработчиками, высокий уровень математического обоснования позволяют утверждать об отсутствии встроенных разработчиками лазеек.

Следовательно, исходя из описанного выше, можно сделать вывод о высоком уровне защиты, обеспечиваемом алгоритмом шифрования AES.

III Открытые вопросы безопасности FIPS-197

В качестве нелинейного преобразования в алгоритме шифрования Rijndael используется одна подстановка (S-блок), применяемая параллельно для всех байтов обрабатываемого блока. В ходе шифрования AES-128 эта подстановка используется 160 раз, и это является единственным нелинейным преобразованием при отображении блока открытого текста в зашифрованный.

При построении подстановки в качестве нелинейной функции было выбрано мультипликативное обращение элемента в поле GF(28). Эта конструкция достаточно хорошо известна в криптографии и гарантирует получение наименьших максимальных значений в таблице распределения разностей и линейных аппроксимаций [9], обеспечивая наилучшие свойства для защиты от дифференциального и линейного криптоанализа.

В работе [31] были исследованы булевы функции, образующие подстановку AES, и обнаружено, что все 8 выходных функций находятся в одном классе относительно некоторого аффинного преобразования. Это означает, что для двух любых выходных битов s_i и s_j подстановки AES существует невырожденная матрица $\mathbf{A}$ и некоторый вектор $\mathbf{B}$, такие, что $s_i(x) = s_j(\mathbf{A}x + \mathbf{B})$. Отсюда следует, что в каждом цикле шифрования AES фактически 128 раз используется одна нелинейная функция с последующими различными аффинными преобразованиями. Существуют и другие подтверждения этого результата с обобщениями аффинного преобразования на все выходные булевы функции цикловой функции AES [32].

Дополнительно в [31] сделан вывод, что операция вычисления обратного элемента в поле GF(28) сохраняет избыточность, и этим свойством обладают все биективные подстановки «8-в-8».

К нынешнему моменту неизвестно ни одной открытой публикации, в которой описана аналитическая атака, каким-либо образом использующая данное свойство AES.

Одним из критериев при построении элементов шифра было использование так называемых ортогональных компонентов (см. п. 1.3), предотвращающих простое алгебраическое описание шифрующего преобразования. В целом, эта задача была решена за счёт использования преобразований в поле GF(2) и GF(28).

В [33] предлагается новый алгоритм шифрования BES (Big Encryption System), построенный на базе AES, но каждый бит AES соответствует одному байту BES. При введении ограничения на множество входных байтов B_i и байтов ключа шифрования K_j, таких, что $B_i, K_j \in \{0,1\}$, существует отображение входных и выходных данных и ключей шифрования алгоритма BES в данные AES. Основное отличие состоит в том, что все операции BES выполняются в одном поле GF(28). Более того, единственное нелинейное преобразование – AES-подстановка – может быть представлена в BES в виде линейного (матричного)

преобразования. Это означает возможность представления цикловой функции BES (и, соответственно, AES) в виде мультипликативного обращения элемента в поле GF(28) и последующего аффинного преобразования: умножения на матрицу $\mathbf{M}_B$ и сложения с вектором-ключом $\mathbf{K}_i$: $\mathbf{X}_{i+1} = F_r^{AES}(\mathbf{X}_i) = \mathbf{M}_B(\mathbf{X}_i)^{-1} + \mathbf{K}_i$, $1 \le r \le 10,12,14$, где все операции выполняются в поле GF(28).

Таким образом, существует возможность представления всех операций AES в одном поле GF(28), и единственную проблему представляет собой отображение данных BES в данные AES.

В настоящее время нет ни одной открытой публикации, в которой описана аналитическая атака, каким-либо образом использующая данное свойство AES.

В работе [34] предлагается использовать для описания подстановки (S-блока) переопределённую систему квадратичных (содержащих в одном терме не более двух переменных) систему уравнений. Далее авторы предлагают построить похожую систему уравнений для всего алгоритма шифрования. Далее формулируется утверждение, что в поле GF(2) сложность решения такой системы является субэкспоненциальной и будет зависеть от количества циклов шифрования. Кроме того, делается вывод, что с увеличением количества циклов стойкость AES увеличивается не экспоненциально.

Авторами не была представлена практическая реализация такой атаки даже для упрощённого варианта AES. Некоторые специалисты, в т. ч. авторы алгоритмов MARS и DES, критически отзываются о корректности описания и возможности реализации данного метода [35, 36].

В [37] выводится формула преобразования в виде цепных дробей, со свойствами, очень близкими к свойствам AES. Преобразование, описывающее полный вариант шифра, содержит 225 термов (в виде цепной дроби). Построив систему из 222 таких уравнений на основе соответствующего количества пар открытых и зашифрованных текстов, криптоаналитик имеет достаточно информации для решения такой системы (с точки зрения теоретико-информационного подхода). На практике в настоящее время неизвестны (по открытым публикациям) методы решения систем уравнений такого типа.

В [38] вводится понятие дуального шифра. С помощью трёх биективных преобразований (для открытого текста, шифртекста и ключа) выполняется преобразование входных и выходных данных алгоритма. Показано [38], что для AES существует множество эквивалентных представлений, выполняющих одно и то же шифрующее преобразование. В [39] приведено 240 различных эквивалентных представлений алгоритма Rijndael. Дуальный шифр эквивалентен AES во всех аспектах. Соответственно, криптоаналитик может выполнять криптоанализ дуального шифра, так же как и разработчик реализовывать дуальный шифр вместо оригинального варианта AES.

В открытых публикациях нет информации об угрозах безопасности в связи с существованием большого количества дуальных шифров AES.

Кроме перечисленных атак, была опубликована работа о возможности выполнения криптоанализа AES с использованием кодов, исправляющих ошибки, исключительно на основе зашифрованных сообщений при фиксации (обнулении) нескольких битов входного блока [40]. Автор метода заявляет об успешном проведении эксперимента по получению 2-х битов секретного ключа по 231 зашифрованным блокам со сложностью примерно 231 (вероятность успеха равна 0,68). Опровержение этого метода было опубликовано в нескольких последующих работах [41, 42]. На наш взгляд, работа носит несколько спекулятивный характер и требует практической проверки украинскими специалистами.

IV Оценка производительности програмных и аппаратных реализаций FIPS-197

Как уже было отмечено, одним из критериев при проектировании Rijndael была простота и минимальная сложность реализации всех компонентов шифра. Авторам алгоритма удалось найти эффективное решение, и в сравнении с другими кандидатами AES и даже более новыми алгоритмами, представленными в конкурсе NESSIE, Rijndael является одним из наиболее производительных шифров, что в значительной степени обусловило победу этого алгоритма во втором туре международного конкурса AES.

В настоящее время существует достаточно большое количество реализаций шифра, сделанных разработчиками разных стран. Лучшие из них использовались в качестве эталонной модели при тестировании производительности 128-битовых симметричных блочных алгоритмов в конкурсе NESSIE [43].

Количество элементарных операций (арифметических инструкций или обращений к таблицам предвычислений) и объём памяти для хранения констант, необходимых для преобразования одного 128-битного блока AES на 32-битном процессоре при зашифровании [43], приведено в табл. 2.

Таблица 2 – Количество элементарных операций и объём памяти для хранения констант, необходимых для преобразования одного 128-битного блока AES

Обращение к таблицам предвычислений	Размер таблиц предвычислений, битов	Количество сдвигов	Количество сложений по модулю 2 (XOR)	Общее количество логических операций
160	8x32	30	120	656

Измерение производительности программных реализаций проводилось на нескольких аппаратных платформах, среди которых в Украине получили распространение x86 под управлением операционных систем Windows и Linux, а также Sparc под управлением Sun Solaris.
При тестировании создавались реализации с использованием нескольких компиляторов при различных комбинациях параметров оптимизации. В качестве итоговой реализации выбиралась наиболее быстродействующая для данной платформы. Отмечается [43], что использование оптимизации под младшие модели процессоров (например, под i386 при работе на Pentium III) в некоторых случаях давало возможность получить более быструю реализацию. Перечень платформ и компиляторов приведен в табл. 3.

Таблица 3 – Перечень платформ и компиляторов, использованных для реализации Rijndael

Название платформы	Windows 2000/P III	Linux/P III	Sparc V9
Использованные компиляторы	Visual C++ (6.0) Intel C++ (6.0) gcc (3.1.1) Borland	gcc (2.95.2, 3.1.1) egcs (2.91.66) Intel C++ (6.0) Borland	SWC 5.1 gcc (3.0.4) cc

Во время тестирования использовалось несколько методик измерения производительности, среди которых, на наш взгляд, наибольший интерес представляет методика измерения количества циклов процессора, затрачиваемых на один байт блока открытого текста при зашифровании. Преимуществом этой методики является независимость от модели и тактовой частоты процессора. В то же время этой информации достаточно для расчёта производительности программной реализации (в Мбайт/с) на конкретной модели процессора данного семейства.

Итоговые характеристики наиболее быстродействующих реализаций под перечисленные платформы приведены в табл. 4. Отсюда следует, что количество тактов процессора, необходимое для шифрования, составляет примерно одну и ту же величину для всех платформ. Этот факт можно объяснить тем, что в алгоритме Rijndael используются максимально простые арифметические операции, которые эффективно кодируются компилятором. Отсюда можно сделать вывод, что производительность реализации криптографических преобразований будет определяться тактовой частотой процессора.

Таблица 4 – Характеристики наиболее быстродействующих реализаций Rijndael

Платформа	Компилятор	Длина ключа	Количество тактов процессора на 1 байт		Количество тактов процессора на вычисление подключей
			зашифрование	расшифрование	
Windows 2000 Pentium III	Visual C++ (6.0)	128	23	23	497
		192	27	27	552
		256	32	32	780
Linux Pentium III	gcc (3.1.1)	128	26	26	504
		192	31	31	601
		256	35	36	949
Sun 450 МГц	Cc	128	21	22	453
		192	25	28	463
		256	29	32	753

Исходя из данных, представленных в табл. 4, можно получить скорость зашифрования (расшифрования) на компьютерах с процессором Intel Pentium 41,5 ГГц порядка 40 Мбайт/с при использовании реализации на языке программирования Си. Если использовать ассемблер, можно получить дополнительное увеличение производительности. В [43] сообщается о достижении производительности, равной 53,3 Мбайт/с.

Таким образом, алгоритм шифрования AES при программной реализации является одним из наиболее быстродействующих, он превосходит по этому показателю другие алгоритмы, которые были протестированы в ходе конкурса NESSIE (DES, TripleDES, Skipjack, IDEA, Camellia, Safer++, Shacal-2 и т. д.).

Кроме того, достигнутый уровень быстродействия программной реализации значительно выше, чем реальная пропускная способность большинства шин ввода/вывода современных компьютеров, в частности, сетевых интерфейсов и каналов подключения жёстких дисков IDE. Это позволяет реализовать высокопроизводительные приложения и системные службы, выполняющие зашифрование и расшифрование прикладных данных, сетевого трафика и потоков обмена с жёсткими дисками с минимальной задержкой и практически в реальном масштабе времени.

В приложениях, требующих чрезвычайно высокого уровня защищённости и надёжности, необходимо использование аппаратных реализаций криптографических алгоритмов. В конкурсе NESSIE выполнялось исследование производительности и сложности реализации криптографических примитивов в виде одной ИМС при использовании различных вариантов изготовления модуля. Основные данные по алгоритму шифрования AES приведены в табл. 5.

Таблица 5 – Производительность аппаратных реализаций AES в виде одной ИМС

Тип аппаратной реализации	Быстродействие	Особенности
FPGA XCV 1000 14 МГц	300 Мбайт/с (37,5 Мбайт/с)	режим с обратной связью
FPGA XCV 1000 32 МГц	1940 Мбайт/с (242,5 Мбайт/с)	режим без обратной связи
ASIC 0,5 мкм	524 Мбайт/с (65,5 Мбайт/с)	–
ASIC 0,5 мкм	5100 Мбайт/с (637,5 Мбайт/с)	конвейеризация
ASIC 0,35 мкм	1950 Мбайт/с (243,75 Мбайт/с)	613000 вентилей

Как можно видеть из табл. 5, высокой производительностью отличается конвейеризированная аппаратная реализация ASIC. Необходимым условием эффективной работы в этом случае является обработка потоков данных с использованием одного ключа шифрования, что обуславливает применение таких решений для защиты передаваемых данных на сетевом и канальном уровне 7-уровневой модели OSI. Производительность решений, наиболее подходящих для обеспечения безопасности пользовательских данных (прикладной и представительский уровень в случае сетевого взаимодействия) сравнима с программной реализацией на современных процессорах.

Первые варианты программных реализаций симметричного блочного шифра Rijndael в АО «ИИТ» были созданы в 1998 году, в начале проведения международного конкурса AES. После проверки соответствия и сравнения с реализациями, доступными в Internet, созданные средства использовались для исследований стойкости, статистической безопасности и производительности Rijndael, алгоритма-кандидата в конкурсе AES [44]. Кроме того, выполнялись исследования возможностей повышения быстродействия за счёт менее сложных эквивалентных представлений внутренних преобразований цикловой функции алгоритма [45], что позволило дополнительно улучшить быстродействие реализации Rijndael на языке высокого уровня на 20%.

Достигнутый к настоящему моменту уровень производительности программных реализаций стандарта шифрования FIPS-197, выполненных в АО «ИИТ», приведен в табл. 6.

Таблица 6 – Производительность программных реализаций FIPS-197, выполненных в АО «ИИТ»

Платформа	Компилятор	Длина ключа	Количество тактов процессора на 1 байт		Количество тактов процессора на вычисление подключей, зашифрование/ расшифрование
			зашифрование	расшифрование	
Windows 2000 Linux Pentium III	Borland gcc (3.1.1)	128	18	17	239/348
		192	21	21	249/432
		256	24	25	351/644

Соответственно, скорость зашифрования (расшифрования) на компьютерах с процессором Intel Pentium 4 1,5 ГГц при использовании реализации на языке программирования Си со вставками на ассемблере составляет величину порядка 85 Мбайт/с.

Сравнивая табл. 4 и 6, можно отметить, что производительность программных реализаций, выполненных в АО «ИИТ», является более высокой, чем тестовые реализации, использованные в конкурсе NESSIE. Это

можно объяснить тем фактом, что украинские специалисты проводили оптимизацию не только за счёт использования эффективных методик программирования, но и за счёт применения более простых криптографически эквивалентных представлений преобразований цикловой функции AES.

После принятия Rijndael в качестве федерального стандарта США FIPS-197, в АО «ИИТ» было выполнено несколько вариантов аппаратной реализации алгоритма. Скорость преобразований при построении аппаратной системы криптографической защиты информации на базе ПЛИС составляет величину порядка 110 Мбайт/с.

Выводы

Приведенные результаты предварительного анализа свойств и исследования стойкости алгоритма симметричного блочного шифрования AES позволяют сделать вывод, что при создании шифра Rijndael использовалась надёжная математическая база, обоснованные критерии оценки и эффективные принципы проектирования. Результаты исследований, полученные независимыми специалистами, позволяют сделать вывод, что FIPS-197 обеспечивает реальную криптографическую стойкость при симметричном блочном шифровании. Для принятия решения об использовании алгоритма в режиме поточного шифра (например, BMGL) и других усовершенствованных режимах, на наш взгляд, необходимы дополнительные исследования.

Таким образом, на современном уровне развития средств и систем криптоанализа шифр AES (FIPS-197) обеспечивает реальную стойкость, является статистически безопасным и, на наш взгляд, ограниченно может применяться в Украине. Алгоритм был подвергнут глубокой экспертизе с привлечением независимых специалистов, обладает приемлемой сложностью криптографических преобразований, может быть реализован аппаратно и программно, для процессоров различных классов.

В дальнейшем, благодаря идеям и принципам, заложенным в алгоритме Rijndael, уровень безопасности шифра может быть дополнительно увеличен. Кроме того, при использовании подобных принципов и новейших результатов в области криптологии, в АО «ИИТ» разработан алгоритм «Торнадо», обеспечивающий ещё более высокий уровень безопасности.

Литература: ***1.*** *National Institute of Standards and Technology, FIPS-197: "Advanced Encryption Standard." Nov. 2001. http://www.nist.gov/aes.* ***2.*** *J. Daemen and V. Rijmen, "AES proposal: Rijndael".http://www.nist.gov/aes.* ***3.*** *J. Nechvatal, E. Barker, et. al. Report on the Development of the Advanced Encryption Standard (AES). Computer Security Division, NIST. http://www.nist.gov/aes.* ***4.*** *D. R. Patel. The AES Winner. http://www.nist.gov/aes.* ***5.*** *NESSIE public report D20. NESSIE Security Report. http://cryptonessie.org.* ***6.*** *NESSIE public report D10. Description of Methodology for Security Evaluation. http://cryptonessie.org.* ***7.*** *И. Д. Горбенко, Л. В. Скрыпник, С. А. Головашич и др. Стандарт симметричного шифрования XXI века: свойства, режимы работы, реализация. Радиотехника. 2001. Вып. 119. С. 22-35.* ***8.*** *J. Daemen, V. Rijmen. The Wide Trail Design Strategy. http://www.nist.gov/aes.* ***9.*** *K. Nyberg, "Differentially uniform mappings for cryptography," Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 55-64.* ***10.*** *N. Ferguson, J. Kelsey, et. al. Improved Cryptanalysis of Rijndael. In Proceedings of FSE'00, no. 1978 in LNCS. Springer-Verlag, 2000.* ***11.*** *J. Daemen. Annex to AES Proposal Rijndael. http://www.nist.gov/aes.* ***12.*** *J. Daemen, V. Rijmen. Rijndael for AES. 3rd AES conference. http://www.nist.gov/aes.* ***13.*** *E. Biham and A. Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, New York, 1993.* ***14.*** *M. Matsui. Linear Cryptanalysis Method for the DES Cipher. Lecture Notes in Computer Science, Advances in Cryptology, in proceedings of Eurocrypt '93, 1993.* ***15.*** *L. R. Knudsen. Truncated and higher order differentials. In B. Preneel, editor, FSE, LNCS 1008. Springer-Verlag, 1995.* ***16.*** *J. H. Cheon, M. Kim, et. al. Improved impossible differential cryptanalysis of Rijndael and Crypton." in Proceedings of ICISC'01, no. 2288 in LNCS. Springer-Verlag, 2001.* ***17.*** *E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. LNCS, Advances in Cryptology, proceeding of EUROCRYPT'93, 1993.* ***18.*** *H. Gilbert, M. Minier. "A collision attack on seven rounds of Rijndael." In Proceedings of the Third Advanced Encryption Standard Conference. NIST. 2000.* ***19.*** *J. Daemen, L. R. Knudsen, V. Rijmen, "The block cipher Square." In Proceedings of Fast Software Encryption '97, no. 1267 in LNCS, Springer-Verlag, 1997.* ***20.*** *L. R. Knudsen, D. Wagner, "Integral cryptanalysis (extended abstract)." In Proceedings of Fast Software Encryption FSE'02, no. 2365 in LNCS, Springer-Verlag, 2002.* ***21.*** *J. Daemen, V. Rijmen. Security of a Wide Trail Design. http://cryptonessie.org.* ***22.*** *Makoto Sugita, Kazukuni Kobara, et. al. Relationships among Differential, Truncated Differential, Impossible Differential Cryptanalysis against Word-Oriented Block Ciphers like Rijndael, E2. http://www.nist.gov/aes.* ***23.*** *Beomsik Song, Jennifer Seberry. Consistent Differential Patterns of Rijndael. http://cryptonessie.org.* ***24.*** *C. Harpes, G. G. Kramer, J. L. Massey. A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma. LNCS, Advances in Cryptology, proceedings of*