Раздел V
Методы и средства криптографии и стеганографии

И.Д. Горбенко, В.И Долгов, Р.В. Олейников, В.И. Руженцев,
М.С. Михайленко, Ю.И. Горбенко
Украина, г. Харьков,
Закрытое акционерное общество «Институт информационных технологий»

РАЗРАБОТКА ТРЕБОВАНИЙ И ПРИНЦИП ПРОЕКТИРОВАНИЯ ПЕРСПЕКТИВНОГО СИММЕТРИЧНОГО БЛОЧНОГО АЛГОРИТМА ШИФРОВАНИЯ

В настоящее время симметричные блочные алгоритмы шифрования являются основным криптографическим средством обеспечения конфиденциальности при обработке информации в современных информационно-телекоммуникационных системах. Кроме того, блочные шифры используются для обеспечения целостности, а также как базовый элемент при построении других криптографических примитивов [1], таких как генераторы псевдослучайных последовательностей (ГПСЧ), поточные шифры и функции хеширования. Уровень стойкости и свойства симметричного блочного алгоритма шифрования, используемого в системе, в существенной степени определяют стойкость криптографической защиты информации, безопасность криптографических протоколов и защищённость информационно-телекоммуникационной системы в целом.

Кроме высокой стойкости, к симметричным блочным алгоритмам шифрования предъявляется требование обеспечения высокого уровня производительности (минимально возможной вычислительной сложности при выполнении шифрования). Принимая во внимание значительные объёмы информации, обрабатываемые информационно-телекоммуникационными системами, это требование является чрезвычайно важным и критичным для эффективного функционирования всей ИТС.

При разработке систем с применением симметричных блочных шифров необходимо учитывать, кроме перечисленных требований, стоимость (простоту построения и эксплуатации) аппаратной и программной реализации алгоритма шифрования.

Таким образом, для современных симметричных блочных алгоритмов шифрования в качестве основных необходимо предъявлять такие общие требования:

1. Обеспечение высокого уровня криптографической стойкости.

2. Высокая производительность при программной, программно-аппаратной и аппаратной реализации.

3. Простота и низкая стоимость программной, программно-аппаратной и аппаратной реализации.

Следует отметить, что указанные требования являются достаточно противоречивыми: например, в большинстве современных алгоритмов увеличение криптографической стойкости требует дополнительных циклов шифрования, что ведет к снижению производительности. Тем не менее, алгоритмы-финалисты международных криптографических конкурсов, таких как AES [2], NESSIE [3-5], CryptRec [6] и других, свидетельствуют о возможности достижения показателей, близких к оптимальным.

Требования к стойкости симметричных блочных алгоритмов шифрования

Как правило, для практически используемых систем криптографической защиты информации, длина сообщения, защищаемого с помощью симметричного блочного шифра, значительно превосходит длину ключа шифрования (энтропия источника сообщений превышает энтропию источника ключа). В этом случае не выполняется критерий безусловной стойкости используемого шифра, и в таких условиях целесообразно введение полиномиального критерия, предполагающего наличие ограничений для вычислительных ресурсов злоумышленника и времени, в течение которого шифр остаётся стойким. Полиномиальный критерий приводит к практическому критерию стойкости – невозможности реализации атаки на шифр в условиях современной вычислительной базы (с учётом прогресса средств вычислительной техники) в течение длительного срока (например, 10^{10} лет).

Стойкость шифра зависит от сложности реализации атаки на симметричный блочный шифр. В качестве показателей сложности, как правило, используют, следующие:

1. Временной – математическое ожидание времени (безопасное время), необходимого для реализации атаки на доступных/перспективных вычислительных средствах.

2. Пространственной сложности - объём памяти, необходимый для выполнения криптографического анализа.

3. Минимально требуемое для успешной реализации атаки количество зашифрованных сообщений, соответствующих им открытых сообщений и т.п.

Анализ показывает, что если хотя бы по одному из указанных показателей реализация атаки на практике невозможна (со значительным запасом стойкости), то алгоритм шифрования можно считать стойким.

Начальная оценка стойкости, как правило, производится по отношению к силовым атакам: полному перебору ключей, атаке по словарю и т.д. При условии обеспечения требуемого уровня стойкости к силовым атакам производится оценка стойкости к аналитическим атакам.

Результаты анализа показали, что для современных симметричных блочных алгоритмов шифрования в качестве критерия стойкости к аналитическим атакам рекомендуется применять следующие:

1. Мощность множества шифрованных/открытых текстов, необходимых для выполнения криптоаналитической атаки, превышает мощность множества допустимых шифрованных/открытых текстов. Например, при длине блока 128 бит (мощность множества шифрованных/открытых текстов 2^{128}) и ключе 256 бит необходимо 2^{170} шифртекстов.

2. Сложность любой аналитической атаки должна быть больше или равна сложности силовой атаки.

Для оценки сложности аналитической атаки по второму критерию, в свою очередь, учитываются два показателя:

- необходимое количество операций шифрования для реализации аналитической атаки (не менее чем при полном переборе ключей);
- требуемый объём памяти для хранения промежуточных результатов аналитической атаки (не менее чем при реализации атаки по словарю на полный шифр).

По крайней мере, сложность атаки по одному из этих показателей должна быть выше, чем у силовой, – только в этом случае шифр является защищённым от криптоаналитической атаки.

Дополнительно, учитывая возможность совершенствования криптоаналитических методов, вводится критерий «запаса стойкости» к аналитическим атакам –

сложность атаки на весь алгоритм должна быть значительно выше сложности силовых атак. Как правило, этот критерий рассматривает версию симметричного блочного алгоритма шифрования с уменьшенным количеством циклов, являющуюся уязвимой против криптографического анализа. Разница в количестве циклов определяет запас стойкости алгоритма к конкретной криптоаналитической атаке (чем больше разница, тем более стойкий алгоритм).

Для оценки криптографической стойкости общей конструкции шифра вводится ещё один критерий, рассматривающий возможность исключения каких-либо операций либо замена их менее сложными операциями (например, на некоторых наборах входных данных операция сложения по модулю 2^{32} близка или эквивалентна операции сложения по модулю 2). В этом случае полноцикловый вариант упрощённого шифра должен оставаться стойким к аналитическим атакам.

Необходимо также учитывать, что большинство современных аналитических атак, прежде всего, таких как дифференциальный и линейный криптоанализ, являются статистическими. При проведении криптоанализа для получения ключа выполняется большое количество шифрований, и на основании криптограмм формируются варианты подключей. При обработке достаточно большой выборки шифртекстов, сформированных на одном ключе, верное значение ключевых бит встречается чаще остальных вариантов. Очевидно, что вероятность нахождения верной пары (предлагающей корректное значение ключа) зависит от статистических свойств шифра, и для увеличения сложности криптоанализа свойства криптограммы должны быть близки к свойствам случайной последовательности.

Поэтому необходимым (но не достаточным) условием стойкости шифра к аналитическим атакам является обеспечение хороших статистических свойств выходной последовательности (шифртекстов).

Для защиты шифра от алгебраических атак необходимо, чтобы не существовало способа практического построения системы уравнений, связывающих открытый текст, криптограмму и ключ шифрования, или не существовало способа решения таких систем в полиномиальное время.

При построении средств криптографической защиты необходимо учитывать возможность организации атак на реализацию (изменение температурного режима электронного устройства, входного напряжения, появление ионизирующего излучения, замер потребляемых токов, ПЭМИН, времени исполнения и т.п.). Такие атаки могут быть эффективны против всех криптографических алгоритмов, и защита от таких атак требует уже инженерных решений при проектировании средств криптографической защиты информации.

В целом, можно сформулировать следующие требования к стойкости современных симметричных блочных алгоритмов шифрования:

1. Обеспечение стойкости к силовым атакам (по временному критерию или критерию требуемого объема памяти для хранения промежуточных результатов).

2. Отсутствие способов построения или решения системы уравнений, связывающей открытый текст, криптограмму и ключ шифрования.

3. Невозможность реализации известных аналитических атак на шифр или их сложность должна быть выше сложности реализации силовых атак (один из следующих критериев: мощности требуемого множества открытых/зашифрованных сообщений; необходимого количества операций шифрования; требуемого объема памяти для хранения промежуточных результатов).

4. Наличие «запаса стойкости» шифра (дополнительных циклов шифрования), обеспечивающего безопасное использование алгоритма в случае совершенствования криптоаналитических атак.

5. Стойкость упрощённого варианта шифра, в котором некоторые операции исключены или заменены более простыми.

6. Обеспечение «хороших» статистических свойств выходной последовательности шифра (криптограммы или гаммы шифрующей), при которых криптограммы и гаммы шифрования практически не отличаются по свойствам от случайной последовательности.

Предлагаемые принципы проектирования перспективного блочного шифра, обеспечивающего высокий уровень стойкости

Учитывая опыт, накопленный при проектировании и анализе блочных симметричных шифров, предлагается использование следующих подходов:

- «консервативное проектирование», использующее только многократно проверенные конструкции и методы;
- стойкость ко всем известным аналитическим атакам;
- формирование большого запаса стойкости, возможность безопасного использования алгоритма в условиях значительного прогресса криптоаналитических техник и/или средств вычислительной техники;
- защита от всех возможных потенциальных уязвимостей алгоритма;
- приоритет стойкости над производительностью;
- ясная структура и «прозрачные» принципы проектирования;
- обеспечение показателей стойкости, превосходящих известные мировые аналоги;
- обеспечение показателей производительности, близких к лучшим мировым решениям.

В основе шифра целесообразно использовать исследованные и многократно проверенные алгоритмы симметричного блочного шифрования, такие как Rijndael [7] и Camellia [8]. По алгоритму Rijndael [9 10] доступно наибольшее количество открытых публикаций исследователей со всего мира, кроме того, алгоритм проверялся специалистами Агентства национальной безопасности США и допущен к защите правительственной информации США всех категорий (по данным сайта НИСТ). На наш взгляд, в качестве основы перспективного блочного шифра целесообразно взять структуру именно алгоритма Rijndael.

При проектировании целесообразно выполнить следующие модификации Rijndael:

- увеличенное количество циклов шифрования (дополнительный запас стойкости);
- использование сложения по разным модулям для введения ключевой информации (защита от алгебраических атак [11], линейного и дифференциального криптоанализа, интерполяционной атаки и т.д.);
- использование нескольких блоков нелинейного преобразования (S-блоков) вместо одного (дополнительная защита от алгебраических атак, улучшение свойств рассеивания шифра – улучшенные статистические свойства, соответственно более высокий уровень стойкости к дифференциальному и линейному криптоанализу и т.п.);
- применение случайно сформированных S-блоков, отобранных по критериям стойкости к дифференциальному, линейному криптоанализу и степени нелинейности булевых функций (в отличие от S-блока Rijndael/Camellia и др. шифров, использующих обращение в поле и соответственно квадратические зависимости между входом и выходом – защита от алгебраических атак);
- введение принципиально новой схемы выработки подключей (защита от всех известных атак на схемы выработки подключей; достаточно высокая произ-

водительность; высокая сложность восстановления мастер-ключа по отдельному подключу).

Все улучшения направлены на увеличение стойкости и перекрытия потенциальных уязвимостей Rijndael.

Построение таблиц подстановки (узлов нелинейного преобразования)

Предлагается применение случайно сформированных таблиц подстановок, отобранных по критериям стойкости к дифференциальному, линейному криптоанализу и степени нелинейности булевых функций. Узлы замены, применяемые в Rijndael/Camellia и др. шифров, используют обращение в поле. Такой S-блок обеспечивает наилучшие показатели с точки зрения ДК/ЛК, но подстановка (S-блок) имеет ярко выраженную математическую структуру и простое алгебраическое представление. Соответственно достаточно серьёзную угрозу наличия уязвимостей шифра к алгебраическим атакам.

Имея многократный запас стойкости к ДК/ЛК (как у Rijndael, так и у перспективного шифра), возможно использование S-блоков с немного худшими показателями S-блока, чем у Rijndael, но в то же время избавиться от явной математической структуры, позволяющей построить квадратичные зависимости между входом и выходом.

Использование случайных S-блоков позволяет избавиться от таких зависимостей (детерминированных) и перейти к вероятностным уравнениям описания подстановки в алгебраических атаках.

Применение нескольких подстановок дополнительно снижает возможность построения и вероятность нахождения верного решения для такой системы уравнений.

Требования к формированию S-блоков перспективного шифра:

- случайная генерация (минимизация вероятности получения строгих математических зависимостей между входными и выходными битами);
- ограничение максимального значения вероятности прохождения разности через подстановку (для перспективного шифра – 2^{-5}, для Rijndael – теоретически достижимый минимум -2^{-6});
- ограничение максимального значения вероятности линейной аппроксимации подстановки (для перспективного шифра – 2^{-2}, для Rijndael – теоретически достижимый минимум -2^{-3});
- нелинейный порядок подстановки (для перспективного шифра – 7, теоретически достижимый максимум).

Кроме того, допускается использование S-блоков в качестве дополнительного устанавливаемого секретного параметра.

Блок линейного преобразования

В качестве блока линейного преобразования используется хорошо проверенное МДР-преобразование, дающее наилучшие свойства рассеивания (распространения разности). Предлагается использовать 64-битовый МДР-код, обеспечивающий полную зависимость каждого бита от входа уже на 2-х циклах шифрования, вне зависимости от размера блока, что даёт лучшие характеристики, чем у Rijndael 256/256, где требуется большее число циклов для распространения разности на весь блок.

Недостаток – менее эффективная реализация на пока используемых 32-битовых процессорах.

Тем не менее, на 64-битовых процессорах, получающих все большее распространение, показатели производительности перспективного шифра близки к Rijndael.

Схема выработки подключей

Схема выработки подключей Rijndael обладает следующими существенными, на наш взгляд, недостатками:

- возможность восстановления мастер-ключа по одному подключу;
- достаточно простые зависимости между подключами (уязвимость к атакам на связанных ключах [12]);
- первый из подключей – мастер-ключ;
- слабое влияние изменений битов мастер-ключа на биты первых подключей (удовлетворительные результаты – только 5-7 подключи);
- использование в схеме разворачивания другой конструкции, отличной от цикловой функции;
- разная сложность генерации последовательности подключей для зашифрования и расшифрования.

В связи с наличием существенных недостатков было принято использовать принципиально новую схему разворачивания.

Требования к схеме разворачивания ключей перспективного алгоритма:

- нелинейная зависимость каждого бита каждого подключа от каждого бита мастер–ключа, соответственно обеспечение всех необходимых лавинных свойств и отсутствие «промежуточных точек»;
- обеспечение стойкости ко всем известным атакам на схемы выработки подключей;
- отсутствие слабых ключей, на которых может произойти ухудшение криптографических свойств шифра;
- невозможность (высокая вычислительная сложность) восстановления мастер-ключа по одному или нескольким подключам;
- простота реализации, использование циклового преобразования шифра;
- вычислительная сложность генерации всех подключей не превышает сложности одной операции шифрования;
- возможность генерации подключей в любом порядке (как для зашифрования, так и для расшифрования).

Режимы работы симметричного блочного шифра

Целесообразно использовать стандартные режимы работы, определённые в NIST SP 800-38A (режимы ГОСТ 28147-89 [13], кроме выработки имитовставки, являются подмножеством этих режимов).

Эти режимы используются более 20 лет (спецификация DES modes of operation), существуют рекомендации по их выбору для конкретных условий применения, и использование этих режимов обеспечивает высокий уровень защиты передаваемых сообщений, свойства режимов хорошо исследованы.

Из-за недостаточной исследованности на текущий момент считаем нецелесообразным использование режима, одновременно обеспечивающим конфиденциальность и целостность сообщений.

Режим обеспечения целостности.

Недостаток стандартного CBC и 4-го режима ГОСТ 28147-89: невозможность обработки сообщения, если его длина не кратна размеру блока шифра (требуется дополнение сообщения, причем имитовставка дополненного сообщения и совпадающего с ним недополненного, такой же длины, совпадает – высокий риск навязывания).

Требования к режиму обеспечения целостности:

- соответствие всем требованиям стойкости, предъявляемым к хэш-функциям;

- возможность обработки сообщений произвольной длины;
- использование одного ключа шифрования.

Большинство известных альтернативных схем используют 2 или 3 ключа шифрования, что является существенным недостатком.

Из известных режимов один ключ используется в OMAC, при этом обеспечивается защита механизма дополнения сообщения, чья длина не кратна размеру блока.

Лучшая атака на OMAC является атакой с выбранными открытыми текстами, когда криптоаналитик выполняет статистический поиск коллизии ($2^{n/2}$ шифрований, где n – размер блока), т.е. фактически теоретический максимум стойкости.

Схема является стойкой, имеет низкую вычислительную сложность, простая в реализации и удобная в использовании.

Таким образом, при использовании предложенных подходов перспективный алгоритм шифрования будет иметь высокий уровень криптографической стойкости и статистической безопасности, обладать высоким уровнем производительности, вместе с тем обеспечивая простоту программной и аппаратной реализации. Полученные показатели стойкости и производительности перспективного шифра позволяют рекомендовать его в качестве замены действующему стандарту ГОСТ 28147-89 [14].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. NESSIE Call for Cryptographic Primitives, Version 2.2, 8th March 2000: http://cryptonessie.org.

2. AES discussion forum: http://aes.nist.gov.

3. New European Schemes for Signatures, Integrity, and Encryption NESSIE: http://cryptonessie.org.

4. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption. Springer-Verlag, Berlin Heidelberg NewYork, etc. 2004, 5. NESSIE public report D20. NESSIE Security Report. http://cryptonessie.org.

6. http://cryptrec.org/ Cryptography Research and Evaluation Committees.

7. *Daemen, J. Rijmen V.* «AES Proposal: Rijndael», AES Round 1 Technical Evaluation CD-1: Documentation, National Institute of Standards and Technology, Aug 1998. http://www.nist.gov/aes.

8. Camelli http://info.isl.ntt.co.jp /crypt /camellia /index.html.

9. National Institute of Standards and Technology, FIPS–197: "Advanced Encryption Standard." Nov. 2001. http://www.nist.gov/aes.

10. *Daemen J. and Rijmen V.*, "AES proposal: Rijndael".http://www.nist.gov/aes.

11. *Courtois N.T., Pieprzyk J.*, Cryptanalysis of block ciphers with overdefined systems of equations. Proceedings of Asiacrypt'02, LNCS. Springer-Verlag, 2002.

12. *Nakahara J. Jr.* Key-Shedule Analysis of AES Candidates //Katholieke Universiteit Leuven, 1999.– P. 143.

13. FIPS 81. DES modes of operation. Federal Information Processing Standards Publication 81, U.S. Department of Commerce / National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1980.

14. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Госстандарт СССР, 1989.

М.Д. Скубилин*, А.В. Письменов*, Ф.Д. Касимов**
Россия, г. Таганрог*, Технологический институт ЮФУ
Азербайджан, г. Баку, Национальная Академия Авиации**

О КРИПТОСТОЙКОСТИ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ

Известные алгоритмы кодирования и декодирования графической информации, передаваемой по открытым каналам связи, недостаточно надежно обеспечивают её конфиденциальность на разумный отрезок времени.