СИНТЕЗ И АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

УДК 621. 391:519.2:519.7

И.Д. ГОРБЕНКО, д-р техн. наук, И.В. ЛИСИЦКАЯ, канд. техн. наук

СТАНДАРТИЗАЦИЯ АЛГОРИТМОВ ШИФРОВАНИЯ. ТРЕБОВАНИЯ К ПРОЕКТУ НАЦИОНАЛЬНОГО СТАНДАРТА БЛОЧНОГО СИММЕТРИЧНОГО ШИФРОВАНИЯ НА СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ КРИПТОГРАФИИ

О стандартах шифрования

Значительная роль алгоритмов шифрования при защите электронной информации в массовом масштабе обусловила необходимость принятия стандартов шифрования, из которых наиболее известным и широко используемым является американский федеральный стандарт DES, принятый в середине 1970-х годов и послуживший аналогом для российского стандарта ГОСТ 28147-89. В настоящее время эти стандарты уже устарели и не соответствуют, как минимум, современным требованиям по скорости шифрования данных [1]. Так, в DES используется 56-битный секретный ключ, который в настоящее время не может обеспечить достаточной стойкости к атаке, основанной на переборе всех возможных значений ключа. Кроме того, для этого стандарта были найдены криптоаналитические атаки, сложность которых оказалась меньше прямого перебора ключей. В [2] отмечается ряд недостатков российского стандарта ГОСТ 28147-89. Так, одним из его недостатков считается сложность его аппаратной реализации. Еще одним существенным недостатком шифра ГОСТ 28147-89 является то, что в нем используются секретные долговременные ключевые данные, которые поставляются "в установленном порядке". В то же время по общепринятым требованиям стойкость алгоритма должна основываться только на секретности легко сменяемого элемента – ключа. К тому же оба шифра обладают низкой стойкостью к атакам на основе случайных аппаратных ошибок. Такая атака является опасной для шифров, применяемых в интеллектуальных электронных карточках. При осуществлении такой атаки предполагается, что нарушитель имеет возможность оказать на шифратор при выполнении процедуры шифрования внешнее физическое воздействие и вызвать одиночные случайные ошибки в регистрах, содержащих данные.

Надо отдать должное тому факту, отмечается в [2], что первый в мире официальный стандарт шифрования был принят в США. Он сыграл важную роль в закреплении мирового лидерства американских производителей криптографических средств защиты информации. Влияние американского стандарта DES на тенденции развития открытой криптографии во всем мире оказалось настолько большим, что в течение первых двадцати лет его применения разработчики блочных алгоритмов шифрования оказались "загипнотизированными" подходами, использованными при разработке DES. Общая схема построения криптосистемы DES стала образцом для подражания. Последнее привело к определенному сдерживанию новых подходов к построению блочных криптосистем, которое отчетливо проявилось в начале 1990-х годов, когда возникла потребность в скоростных методах шифрования, ориентированных на программную реализацию.

В 1998 – 2000 гг., когда стало окончательно ясно, что алгоритм DES уже исчерпал свои возможности, США, сохраняя первенство в этом направлении, провели международный открытый конкурс на стандарт 21-го столетия (продвинутый) – Advanced Encryption Standard (AES). Конкурс успешно завершился. Победителем стал шифр Rijndal бельгийских разработчиков. Сильную конкуренцию победителю составили шифры RC-6 и Tofish. Вслед за этим конкурсом был объявлен аналогичный европейский конкурс (NESSI). Еще раз важно отметить, что в процессе открытого обсуждения проектов предлагаемых шифров и примитивов, их всестороннего анализа и сравнения был осуществлен существенный прорыв не только в

теории криптографии, но и в развитии новых подходов к разработке и построению шифров, а также в развитии практических методов криптоанализа.

Конечно, через распространение своих алгоритмов шифрования и средств ЗИ ведущие страны закрепляют позиции на рынке продуктов и услуг в области информационной безопасности, а также усиливают влияние и приобретают в определенной степени возможность контроля защищенности информационного ресурса других стран.

Поэтому архиважной задачей для Украины является быстрое освоение современных технологий криптографической защиты информации, выход на уровень создания и принятия собственных или гармонизированных международных стандартов, что, несомненно, способствовало бы укреплению ее суверенитета и независимости. Проблема разработки скоростных шифров, соответствующих современным мировым требованиям и тенденциям, уже декларирована и в Украине [2], и работы в этом направлении уже развернуты.

Первые уроки

Начнем с того, что 30 июня 2006 г. на сайте ДСТЗІ Украины появилось официальное объявление о проведении конкурса по выдвижению кандидатов на национальный стандарт шифрования [3]. В процессе проведения конкурса было рассмотрено пять предложений, из которых на окончательное рассмотрение было представлено четыре (шифры ADE, Калина, Мухомор и Лабиринт). В отборе и анализе представленных решений приняли участие ученые и разработчики коллектива ЗАО "ИИТ", которые представили на конкурс два своих предложения (Калина, Мухомор). Конечно, работа над экспертизой проектов потребовала освоить и уже имеющийся международный опыт и форсировать разработку собственных подходов и методик, позволяющих ускорить процесс анализа и принятия решений. Анализ представленных на украинский конкурс решений показал, что шифры Калина и Мухомор [4, 5] (можно здесь отметить и другие предложения – ADE и Лабиринт [6, 7]) не уступают практически по всем показателям, в том числе и по стойкости к атакам линейного и дифференциального криптоанализа победителю конкурса AES – шифру Rijndael. Тем не менее, по результатам конкурса принято решение остановиться на общепризнанном мировом стандарте Fips-197 (AES). Национальные предложения оказались либо слишком близкими по конструкции к мировому лидеру, либо недостаточно прозрачными с точки зрения ожидаемых показателей стойкости по сравнению с мировым авторитетом.

Действительно, при принятии решений по конструкции БСШ разработчики находились под сильным влиянием конструкции уже признанной мировым сообществом

Шифр Калина по существу явился подражанием мировому лидеру. При его построении пошли по простому пути – не меняя принципиальных решений внести изменения, позволяющие перекрыть к тому времени уже обнаруженные потенциальные слабости шифра Rijndael, заключающиеся в его заметной алгебраичности (его прозрачная сбалансированная конструкция допускала алгебраическое описание [8]). Поэтому было принято решение заменить S-блоки, поддающиеся алгебраическому описанию, случайными и дополнительно ввести сложение с цикловыми подключами по еще одному модулю (наряду с операцией XOR, как это сделано в оригинале, ввести и операцию сложения по mod 2^{32}). Позже стало известно, что близкие решения были приняты и в шифре Anubis, представленном на конкурс NESSIE [9].

При построении шифра Мухомор использованы решения, близкие к другой уже достаточно хорошо известной конструкции шифра FOX [10]. Скелет цикловой функции строился на основе использования схемы Лея – Массэя, а внутренние преобразования цикловой функции, как и в шифре FOX, строились с применением матричного умножения выходов линейки S-блоков (SL-преобразование).

Оказались невостребованными и другие украинские предложения (шифры ADE и Лабиринт).

Отметим, что все указанные четыре шифра оказались близкими по показателям стойкости и быстродействию шифру Rijndael (Лабиринт медленнее Rijndael-я). По крайней мере,

два из предложений считались не уступающими ничем Rijndael-ю. Тем не менее, окончательное решение, как уже было отмечено выше, оказалось в пользу мирового лидера (стандарта FIPS-197).

Какие уроки можно вынести из прошедших событий:

1. Решения, представленные на украинский конкурс, не имели заметных преимуществ по сравнению с шифром Rijndael, или научно методический аппарат, которым владели разработчики, не позволил им обосновать преимущества своих решений;

2. Стратегия подражания, когда разработки в значительной степени повторяют известные решения, себя не оправдывает, т.е. необходимо искать конструкции, обладающие большей оригинальностью и ощутимыми преимуществами (испытание временем тоже очень серье зный критерий при анализе альтернатив);

3. Конкурировать с предложениями, прошедшими экспертизу специалистов мирового класса, очень трудная задача. Необходимо выходить со своими разработками на более высокие уровни экспертизы и их анализа, в частности нельзя игнорировать участие в международных конкурсах и проектах.

4. Быстро хорошего решения не найде шь. Должен идти непрерывный процесс накопления и совершенствования перспективных разработок и решений.

Но это все уроки на будущее. А пока остае тся работа по углубле нному изучению опыта и достижений современной криптографии и поиска своего вклада в теорию и практику блочного симметричного шифрования, дальнейшее осмысление обширного набора требований к национальному стандарту и поиска путей эффективного их выполнения.

Требования к современным блочным симметричным шифрам (БСШ)

В этом разделе мы хотим привести требования к перспективным БСШ, которые в концентрированной форме изложены в положении прошедшего украинского конкурса [2]. Конечно, эти требования стали результатом изучения и обобщения мирового опыта в этом направлении, в частности прошедших конкурсов AES, NESSIE, CRYPTREC, и поэтому нет необходимости возвращаться к анализу известных документов.

Следуя [2], представим основное его содержание. Можно отметить, что изложенные требования можно свести к следующим основным:

1. Параметры криптоалгоритма:

- криптоалгоритм должен быть симметричным блоковым;
- размер блока данных – 128, 256, 512 бит;
- размер разового (сеансового) ключа – 128, 256, 512 бит.

2. Принципы построения:

– способность противостоять известным методам криптографического анализа и иметь запас стойкости с уче том тенденций развития средств электронной вычислительной техники и криптологической науки;

- применяемые криптографические преобразования должны базироваться на наде жной и прозрачной математической базе и не иметь встроенных лазеек;
- скорость криптоалгоритма должна быть не меньше, чем скорость существующего государственного стандарта шифрования (а еще лучше быть того же порядка, что и у Fips-197).

3. Реализация алгоритма:

– криптоалгоритм должен быть ориентирован на возможности реализации на 32- или 64-разрядных процессорах;

– определе нные в криптоалгоритме операции должны допускать эффективную программную и аппаратную реализации;

– необходимый для работы объе м памяти должен учитывать возможности реализации алгоритма в микроустройствах;

– должна быть предусмотрена возможность распараллеливания основных операций (алгоритмов зашифрования, расшифрования и разворачивания ключей).

Ключевая система:

– криптоалгоритм может предусматривать наличие долговременного ключа;

– длина синхропосылки – не меньше 64 битов.

Режимы шифрования:

В криптоалгоритме должны быть предусмотрены следующие режимы шифрования:

– простая замена;

– сцепление блоков шифрованного текста;

– обратная связь по входу;

– обратная связь по выходу;

– режим выработки гаммы ("длинного цикла").

Как видно из представленного списка требований, в них учтены материалы и результаты прошедших международных конкурсов и имеющийся собственный опыт эксплуатации существующего стандарта. Сегодня уже можно отметить работу по уточнению и доработке этих требований.

В частности, просматривается возрастание технологических требований к алгоритмам шифрования [3]. Ставится задача – при сохранении требования обеспечения гарантированной стойкости реализовать высокую скорость шифрования как при программной (более 100 *Мбит/с*), так и при аппаратной (более 1000 *Мбит/с*) реализациях. При этом ставится условие, чтобы устройства шифрования по своей стоимости были доступными массовому пользователю. Дополнительно актуализируется необходимость обеспечения стойкости алгоритмов к ряду нетрадиционных атак, например к атаке на основе случайных аппаратных ошибок.

Некоторые полезные результаты пройденного пути

Решение задач, связанных с разработкой современных стандартов шифрования, очевидно, выдвигает на первый план владение современными методами оценки эффективности разрабатываемых и предлагаемых решений, важнейшей компонентой которых является владение методами криптоанализа

Конечно, основная (определяющая) компонента требований к блочным симметричным шифрам состоит в обеспечении высоких показателей криптостойкости. Здесь мы хотим отдельно остановиться на обеспечении стойкости к атакам дифференциального и линейного криптоанализа, считающимся наиболее мощными и наиболее опасными.

Следует отметить, что работа над представленными на украинский конкурс проектами не прошла даром. Получен опыт не только в разработке современных шифров, но и в освоении всего научно-методического аппарата, применяемого для оценки и сравнения между собой различных алгоритмов шифрования, выполнения проверки свойств и показателей стойкости алгоритмов шифрования за короткий период их анализа.

Сегодня уже можно сказать, что итогом прошедшего времени является предложенная и проверенная в действии новая ускоренная методика криптоанализа современных шифров, основанная на разработке и изучении свойств уменьшенных версий (моделей) шифров [11].

Выявлены недостатки существующей методики оценки стойкости блочных шифров к атакам дифференциального и линейного криптоанализа [12].

Разработана новая идеология (система взглядов) к оценке стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа, обладающая более высокой объективностью и точностью оценок [13].

Установлено, что показатели стойкости блочных шифров (максимальные значения полных дифференциалов и линейных корпусов) определяются не свойствами нелинейных преобразований (S-блоков), применяемых в современных шифрах, как это пропагандируется во многих зарубежных работах, а свойствами случайных подстановок, к которым приходят со-

временные шифры в процессе выполнения многоцикловых процедур шифрования [13]. Для каждого шифра существует свой переходный процесс прихода к случайной подстановке.

В результате появляется возможность выполнить сравнительную оценку шифрующих преобразований (шифров) по числу циклов шифрования, необходимых для "прихода" шифра к показателям случайной подстановки. Например, шифр семейства IDEA NXT требует для "прихода" к асимптотическому (установившемуся) значению полного дифференциала на два цикла преобразований больше, чем это требуется для шифра Rijndael. Поэтому (при прочих равных условиях) шифр Rijndael следует считать более совершенной конструкцией.

Этот критерий предлагается ввести для оценки эффективности конструкций цикловых преобразований. Возможно, что из всех вариантов построения цикловых конструкций та будет перспективнее, которая обеспечит переход к асимптотическому значению максимума полного дифференциала и асимптотическому значению максимума линейного корпуса за меньшее число циклов шифрования. Естественно, такое сравнение полноразмерных шифров неосуществимо. Однако его можно выполнить на малых (масштабированных) версиях шифров в рамках уже отмеченной выше ускоренной методики криптоанализа [11].

Заключение

Действительно, разработка и принятие нового стандарта блочного симметричного шифрования является для Украины одной из центральных задач в области криптографии. При ее решении необходимо исходить из двух альтернатив: создание оригинальной конструкции или гармонизация на основе лучших международных стандартов.

Мировой опыт разработки и принятия новых стандартов и результаты проведенных международных конкурсов позволили сформировать систему критериев (требований), которым должен удовлетворять современный блочный симметричный шифр.

Уже имеется опыт построения шифров, претендующих стать национальными стандартами, однако пока не удалось (а может, и не удастся) предложить конструкции, обладающие существенными преимуществами по сравнению с имеющимися решениями (алгоритмами шифрования), хотя следует отметить, что уже имеются прогрессивные решения в плане повышения быстродействия.

Одним из перспективных направлений поисков прогрессивных решений может стать разработка более эффективной конструкции циклового преобразования, позволяющего за меньшее число циклов шифрования реализовать переход к состоянию, обладающему показателями случайной подстановки.

Список литературы: 1. *NESSIE* security report // http:// www. Cryptonessie. Org / NES/DOC/ENS/WPS/D20/2, 2003. 2. *Молдавян А.А.* и др Криптография: скоростные шифры. – СПб. : БХВ-Петербург, 2002. – 496 с. 3. *Положення* про проведення відкритого конкурсу криптографічних алгоритмів. http://dstszi.gov.ua/dstszi/control/uk/ publish /, 2006. 4. *Горбенко І.Д.* Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації / Горбенко І.Д. Долгов В.І., Олейніков Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Тоцкій О.С., Казьміна С.В. // Прикладна радіоелектроніка. – 2007. – Т.6. – № 2. – С. 195-208. 5. *Горбенко І.Д.* Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація / Горбенко І.Д., Бондаренко М.Ф., Долгов В.І., Олійников Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Олешко О.І., Кузьміна С.В // Прикладная радиоэлектроника. – Харьков : ХТУРЭ. – 2007. – Т. 6, №2. – С. 147-157. 6. *Головашич С.А.* Спецификация алгоритма блочного симметричного шифрования «Лабиринт» // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. – Т. 6, №2. – С. 230-240. 7. *Кузнецов А.А.* Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) / Кузнецов А.А., Сергиенко Р.В., Наумко А.А. // Прикладная радиоэлектроника. – Харьков : ХТУРЭ. – 2007. – Т. 6, №2. – С. 241–249. 8. *Nicolas Courtois.* General Principles of Algebraic Attacks and New Design Criteria for Components of Symmetric Ciphers. In H. Dobbertin, V. Rijmen, and A. Sowa, editors, Fourth Conference on the Advanced Encryption Standard – AES4, volume 3373 of Lecture Notes in Computer Science, pages 67–83. Springer-Verlag, 2004. 9. *P. Barreto, V. Rijmen.* The Anubis Block Cipher, Submission to the NESSIE Project, 2000. 10. *P. Junod and S. Vaudenay.* FOX: a new family of block ciphers. In H. Handschuh

and A. Hasan, editors, Selected Areas in Cryptography: 11th International Workshop. SAC 2004. Waterloo, Canada, August 9-10, 2004. Revised Selected Papers, volume 3357 of Lecture Notes in Computer Science, pages 114–129. Springer-Verlag, 2004. 11. *Долгов В.И.* Подход к криптоанализу современных шифров / Долгов В.И., Лисицкая И.В., Олейников Р.В. // Материалы второй международной конференции "Современные информационные системы. Проблемы и тенденции развития". – Харьков-Туапсе, Украина, 2–5 октября. – 2007. – С. 435-436. 12. *Лисицкая И.В.* Об участии S-блоков в формировании максимальных значений дифференциальных вероятностей блочных симметричных шифров / Лисицкая И.В., Казимиров А.В. // Proceedings International Conference SAIT 2011. – Kyiv, Ukraine, May 23-28, 2011. – С. 459. 13. *Горбенко І.Д.* Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко І.Д., Долгов В.И., Лисицкая И.В., Олейников Р.В. // Прикладная радиоэлектроника. – 2010. – Т. 9. № 3. – С. 212-320.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 11.07.2011