УДК 004.056.55

Александр Кузнецов[1], Бахытжан Ахметов[2], Анар Ташимова[3]
[1] Харьковский национальный университет имени В.Н. Каразина, Украина
[2]Казахский национальный исследовательский технический университет имени К.И. Сатпаева, Республика Казахстан
[3]Актюбинский региональный государственный университет имени К.Жубанова

МАТЕМАТИЧЕСКИЕ МОДЕЛИ КЛЮЧЕВОГО РАСПИСАНИЯ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Исследуются комбинаторные свойства ключевого расписания блочных симметричных шифров в предположении, что цикловые (раундовые) ключи формируются случайно, равновероятно и независимо друг от друга. Для абстрактного описания такого формирования используется модель случайной однородной подстановки. Результаты имитационного моделирования подтверждают достоверность и обоснованность полученных аналитических выражений.
Ключевые слова: ключевое расписание, цикловые ключи, комбинаторные свойства, блочные симметричные шифры.

Alexandr Kuznetsov, Bakhytzhan Akhmetov, Anar Tashimova

MATHEMATICAL MODELS OF THE KEY SCHEDULE OF BLOCK SYMMETRIC CIPHERS

We investigate combinatorial properties of the block symmetric ciphers key schedule in the assumption that the cyclic (round) keys are generated randomly, with equal probability and independently of each other. The model of random homogeneous substitution is used for an abstract description of this formation. The simulation results confirm the accuracy and validity of these analytical expressions.
Key words: key schedule, cyclic keys, combinatorial properties, block symmetric ciphers.

Существование и устойчивое развитие современного независимого государства неразрывно связано с обеспечением информационной безопасности, в том числе в коммерческих и государственных структурах, банковской системе, военно-промышленном и топливно-энергетическом комплексах, в телекоммуникационных и информационно-управляющих системах различного назначения. Для защиты информации в современных информационно-телекоммуникационных системах используется шифрование, под которым понимают обратимое криптографическое преобразование открытых данных для сокрытия их смыслового содержания от неуполномоченного пользователя (злоумышленника). Взаимно-однозначные процессы зашифрования-расшифрования блоков открытого текста (англ. plaintext) и блоков шифртекста (англ. ciphertext) параметризируется ключевыми данными, которые для симметричных криптопреобразований совпадают [1].

Большинство блочных симметричных шифров (БСШ) являются *итеративными* [1], в которых шифрование реализуется посредством циклически повторяющихся обратимых раундовых функций (рис. 1). На каждой итерации БСШ для параметризации раундовых преобразований используются т.н. *раундовые (цикловые) ключи* $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$. Они формируются посредством расширения (планирования, расписания) мастер-ключа $K^{(x)}$ (англ. keyscheduling) [1].

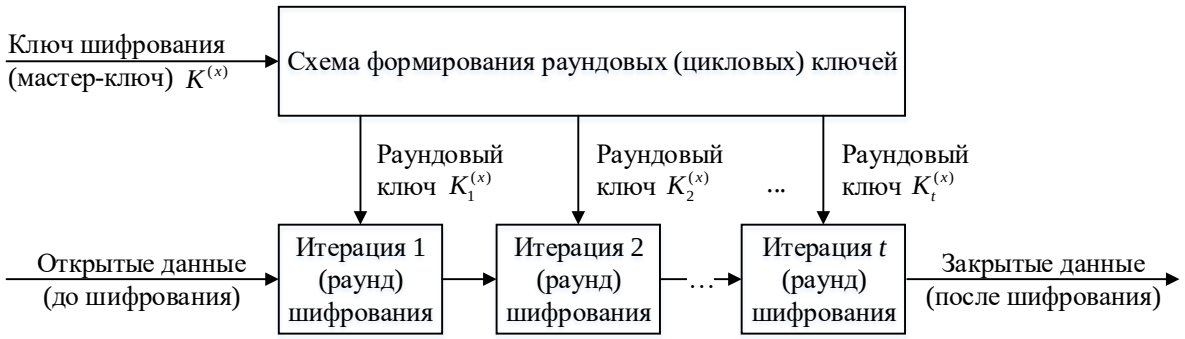

Рис. 1. Структурная схема итеративного блочного шифра

Структура ключевого расписания итеративных БСШ, простота формирования и/или взаимозависимость раундовых ключей, лежат в основе известных атак на схемы разворачивания. В частности, наибольшее развитие получили т.н. *сдвиговые атаки* (англ. slideattack) [2 - 4], *атаки на связанных ключах* (англ. related-keyattack) [5 - 7] и пр. [1]. В простейшем случае схема разворачивания может состоять в повторении мастер-ключа для каждого раунда. Подобный подход использовался при формирования цикловых ключей в советском алгоритме симметричного криптопреобразования ГОСТ 28147-89, являющегося и стандартом шифрования Украины ДСТУ ГОСТ 28147:2009 [1]. Однако в случае, когда на вход каждой раундовой функции (см. рис. 1) подается некоторый ключ, одинаковый для всех раундов, шифр становится уязвимым к сдвиговой атаке [2, 3]. К этому простейшему случаю легко сводится вариант, когда функция разворачивания предполагает циклическое повторение некоторого набора раундовых ключей (шифры с раундовым самоподобием, англ. roundself-similarityciphers) [4].

Для противодействия криптоаналитическим атакам на ключевое расписание современные БСШ используют усложненные схемы разворачивания раундовых ключей, построенные, например, на использовании шифроподобных преобразований. К числу таких БСШ следует отнести, в первую очередь, национальный стандарт США FIPS-197 (AES) [8, 9], принятый в 2001 году и являющийся, де-факто, международным алгоритмом, получившим наибольшее распространение в современных протоколах безопасности. Ключевое расписание БСШ AES представляет собой линейный массив 4-х байтовых слов. Первые элементы массива содержат мастер-ключ шифрования, остальные определяются рекурсивно посредством суммирования по модулю два предыдущих элементов. Для некоторых позиций массива дополнительно применяются шифроподобные преобразования, в частности, нелинейная подстановка блока данных, циклический сдвиг и пр. [8, 9]. В результате формируемая последовательность раундовых ключей $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$ нелинейно зависит от исходного мастер-ключа $K^{(x)}$, и эта дополнительно внесенная нелинейность позволяет эффективно противостоять сдвиговым атакам на ключевое расписание [1].

Атаки на связанных ключах впервые предложены в [5] и получили дальнейшее развитие в [6, 7]. В частности, в работе [7] предложена первая криптоаналитическая атака на основе связанных ключей на полнораундовые шифры AES-192 и AES-256 (варианты FIPS-197 с длиной ключа 192 и 256 бит). Следует отметить, что приведенные в [7] атаки эффективнее полного перебора мастер-ключей, т.е. можно с уверенностью утверждать о реальном снижении стойкости стандартизированного криптоалгоритма.

Таким образом, атаки на ключевое расписание непрерывно совершенствуются и их возможное использование представляет реальную угрозу безопасности современным информационным системам и технологиям [1 - 7]. Перспективные БСШ должны эффективно противостоять атакам на ключевое расписание, схема разворачивания не должна содержать уязвимостей, обусловленных простотой

формирования и взаимной зависимостью цикловых ключей. Фактически, речь идет о таком «идеальном» разворачивании раундовых ключей, при котором каждый элемент последовательности $K_1^{(x)}, K_2^{(x)}, ..., K_t^{(x)}$ формируется случайно, равновероятно и независимо от других цикловых ключей. Только в этом случае можно с уверенностью утверждать о бесполезности атак на ключевое расписание, т.к. каждый раунд БСШ параметризируется случайно выбранным значением и будет функционировать независимо от других итераций схемы шифрования (см. рис. 1).

Для описания схемы разворачивания раундовых ключей в данной работе использовалась абстрактная модель случайной подстановки, параметризированная значением мастер-ключа шифрования. Полученные с ее помощью аналитические соотношения позволяют оценить вероятностные свойства цикловых ключей БСШ. В частности, вероятность кратного совпадения раундовых ключей при заданном числе реализаций случайной однородной подстановки (заданном числе мастер-ключей) определяется по формуле Бернулли. Это соотношение дает оценку вероятности такого события, когда на всем множестве мастер-ключей конкретный раундовый ключ будет сформирован хотя бы один раз, т.е. позволяет оценить среднее число различных раундовых ключей на выходе схемы формирования. Последний результат обобщен на последовательности раундовых ключей произвольной длины, т.е. в рамках принятой модели удается получить численные оценки вероятностных свойств всех элементов ключевого расписания БСШ.

Литература

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: Підручник для вищих навчальних закладів. – Харків: Вид-во «Форт», 2013. – 880с.
2. Biryukov A., Wagner D. Slide Attacks (англ.) //Fast Software Encryption. 6th International Workshop, FSE’99 Rome, Italy, March 24–26, 1999 Proceedings. - Springer Berlin Heidelberg, 1999. - С. 245-259.
3. Chalermpong Worawannotai, Isabelle Stanton A Tutorial on Slide Attacks (англ.). [Электронный ресурс] – Режим доступа: http://www.eecs.berkeley.edu/~isabelle/slideattacks.pdf.
4. Biryukov A., Wagner D. Advanced Slide Attacks (англ.) // Advances in Cryptology - EUROCRYPT 2000. International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14-18, 2000 Proceedings. - Springer Berlin Heidelberg, 2000. - С. 589-606
5. Biham E. New types of cryptanalytic attacks using related keys (англ.) // Springer-Verlag : журнал. - 1994. - № 4. - С. 229-246.
6. Ciet M., Piret G., Quisquater J.-J. Related-Key and Slide Attacks: Analysis, Connections, and Improvements (Extended Abstract). // http://citeseer.ist.psu.edu – 2002 – Universite catholique de Louvain, Louvain-la-Neuve, Belgium
7. Biryukov A., Khovratovich D. Related-Key Cryptanalysis of the Full AES-192 and AES-256 (англ.) // Springer Berlin Heidelberg : журнал. - 2009. - С. 1-18.
8. FIPS-197: Advanced Encryption Standard (AES) // National Institute of Standards and Technology. - 2001. [Электронный ресурс] – Режим доступа: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
9. FIPS-197: Advanced Encryption Standard (AES) // National Institute of Standards and Technology. - 2001. [Электронный ресурс] – Режим доступа: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.