Г.2 Вычислительный метод синтеза регулярных нелинейных узлов замен с использованием недвоичных криптографических функций

Рассматриваются вычислительные методы синтеза регулярных нелинейных узлов замен для симметричных криптографических алгоритмов преобразования информации. С использованием математического аппарата корреляционного и спектрального анализа обосновываются критерии поиска недвоичных криптографических функций для нелинейных узлов замен симметричных криптоалгоритмов. На основе усовершенствованных весовых коэффициентов ценовых функций поиска предлагается дальнейшее развитие метода имитации отжига (Simulated Annealing), исследуется эффективность предлагаемого подхода.

перечень ключевых слов: S-блок, вычислительный метод синтеза, метод имитации отжига, весовые коэффициенты, нелинейность, автокорреляция, криптографическая функция

Постановка проблемы в общем виде и анализ литературы

Нелинейные узлы замен (S-блоки) являются ключевым элементом современных симметричных криптографических алгоритмов, среди которых наиболее известными являются стандарты блочного симметричного шифрования (БСШ) DES, ГОСТ-28147-89 и AES [1].

S-блок nxm представляет собой нелинейную функцию отображения n входных бит в m выходных. В случае, когда на выходе S-блока появляются все возможные m-битные значения и каждое выходное значение равновероятно, S-блок называют регулярным. Регулярность S-блока является обязательным условием для его использования в современных БСШ. Кроме того, для обеспечения устойчивости БСШ к атакам дифференциального и линейного криптоанализа используемые узлы замен должны удовлетворять требуемым показателям нелинейности и автокорреляции [2].

Вычислительным методам синтеза криптографически стойких регулярных узлов замен посвящено множество работ [2-8]. Однако, как показал проведенный анализ, показатели формируемых S-блоков далеки от оптимальных, с увеличением их размерности некоторые методы становятся вычислительно нереализуемыми [3, 9]. Перспективным направлением исследований является использование математического аппарата недвоичных криптографических функций, что, как показано в данной работе, позволяет синтезировать регулярные нелинейные узлы замен с требуемыми показателями нелинейности и автокорреляции.

В данной работе разрабатываются новые критерии вычислительного поиска криптографически стойких S-блоков. На основе усовершенствованных весовых коэффициентов ценовых функций поиска предлагается дальнейшее развитие метода имитации отжига (Simulated Annealing). В основу предлагаемых функций стоимости положены спектральные и корреляционные свойства недвоичных криптографических функций, математический аппарат которых предложен в [10].

Вычислительный метод синтеза регулярных нелинейных узлов замен

Анализ открытой литературы показал, что на сегодняшний день существует ряд вычислительных методов синтеза регулярных нелинейных узлов замен, среди которых [2-8]: побитовые методы (bit-by-bit methods), методы случайной генерации с фильтрацией (random generation), метод градиентного подъема (hill climbing), генетические алгоритмы (genetic algorithms), метод имитации отжига (simulated annealing), метод дифференциальной эволюции (differential evolution), метод оптимизации роем частиц (particle swarm optimization) и др. На наш взгляд наиболее эффективным методом синтеза регулярных S-блоков является метод имитации отжига SA. Так, например, на основе проведенных в работах [6, 13] сравнений показано, что использование метода имитации отжига позволяет реализовать вычислительный поиск криптографических функций с лучшими на сегодняшний день показателями. Описание и алгоритм метода приведены ниже [6].

Поиск начинается с некоторого начального состояния . Параметр T – некий контрольный параметр, известный как температура. T инициализируется высокой температурой T_0 и постепенно снижается. При каждом значении температуры, выполняется определенное число MIL (Moves in Inner Loop, шагов во внутреннем цикле) шагов к новым состояниям. Состояние-кандидата Y выбирается случайным образом из соседей N(S) текущего состояния. Вычисляется изменение значения функции cost, $\delta = cost(Y) - cost(S)$. Если значение cost(S) улучшается (т.е. для задачи минимизации), тогда выполняется шаг относительно этого состояния (S = Y); в противном случае – он выполняется с некоторой вероятностью. Чем хуже шаг, тем меньше вероятность того, что он будет принят; чем ниже температура T, тем менее вероятно, что ухудшающий шаг будет принят. Вероятностное принятие решения определяется генерацией случайного числа U в интервале (0…1) и выполнением указанного ниже сравнения.

Вначале температура высокая и принимается почти каждый шаг. Это сделано для того, чтобы поиск носил не локальный, а глобальный характер. По мере того как температура уменьшается, становится все более трудно принимать ухудшающие шаги. В конце концов, допускаются только улучшающие шаги и процесс застывает. Алгоритм прерывается, когда встречается критерий остановки. Общий критерий остановки (который и был применен в нашей работе) – остановка поиска при достижении заданного числа MaxIL внутренних циклов, либо когда было выполнено некоторое максимальное число MUL последовательных непродуктивных внутренних циклов (т.е. без единого принятого шага). При этом лучшее достигнутое состояние сохраняется, поскольку поиск может выйти из него и впоследствии не найти состояние с подобными показателями. В конце каждого внутреннего цикла температура понижается. В нашей работе использовалось геометрическое охлаждение – умножение на константу охлаждения в интервале (0…1).

Соседей функции f можно определить следующим образом. Функция g находится по соседству с функцией f, если:

Алгоритм имитации отжига SA

```
S = S0;
T = T0;
repeat {
    for (int i = 0; I < MIL; i++)
    {
    выбрать Y  N(S);
     = cost(Y) - cost(S);
    if ( < 0) then S = Y;
    else сгенерировать U = U(0,1);
    if (U < exp(-/T)) then S = Y;
    }
    T = T x;
}
until (критерий остановки не достигнут).
```

Поиск начинался со сбалансированной, но при этом случайной функции. Один шаг алгоритма меняет местами два отличных элемента таблицы истинности функции, сохраняя ее сбалансированность.

Рассмотрим процедуры формирования функций стоимости cost (ценовых функций), используемые для синтеза S-блоков через спектральные характеристики булевых функций, введем соответствующие функции стоимости для синтеза S-блоков через спектры недвоичных криптографических функций.

Пусть функция задает S-блок размерности nxm. Пусть для , - линейная комбинация m выходов S-блока F. Тогда - значения преобразования Уолша-Адамара и значения автокорреляции для каждой булевой функции.

Поскольку нелинейность булевой функции , то задача повышения нелинейности может быть представлена как задача минимизации абсолютного максимального значения коэффициента Уолша-Адамара. Изначально в задачах синтеза S-блоков по критерию высокой нелинейности для метода имитации отжига использовалась следующая функция стоимости [6]:

.

Поскольку задача понижения автокорреляции представляется как задача минимизации максимального значения автокорреляционной функции, то cost функция в дальнейших исследованиях приняла следующий вид [6]:

.

Обычно в многокритериальных задачах применяется следующий подход: вычисляется сумма отдельных cost функций (по различным критериям), умноженных на весовые коэффициенты. Тогда cost функция в задаче синтеза S-блока с высокой нелинейностью и низкой автокорреляцией принимает вид [6]:

Далее были разработаны улучшенные функции, которые основывались на следующем положении.

Известно, что равенство Парсеваля

ограничивает значением равным как минимум $2^{n/2}$. Данная граница достигается тогда, когда выполняется равенство для каждого ω. Когда значение некоторого коэффициента меньше этой

идеальной границы, теорема Парсеваля утверждает, что другие значения коэффициентов должны быть выше этой границы. Таким образом, попытка ограничить отдаленность абсолютных значений коэффициентов Уолша-Адамара от данной границы является возможным средством достижения высокой нелинейности. Спектры некоторых функций содержат все значения (по модулю), равные этой идеальной границы. Такие функции называются бент-функциями.

Помимо обладания наивысшей возможной нелинейностью эти функции имеют нулевую автокорреляцию. Следовательно, функция стоимости

(1)

является возможным подходом к оптимизации нелинейности и автокорреляции. В виду несбалансированности бент-функций приведенная функция стоимости cost может быть улучшена для нахождения сбалансированных криптографических функций. В [6] было введено обобщение функции стоимости (1), которое приняло следующий вид:

. (2)

Параметры X и R, называемые весовыми коэффициентами, обеспечивают свободу для экспериментирования и поиска оптимальных значений.

По аналогии с функциями стоимости относительно спектра Уолша-Адамара вида (2), функции стоимости относительно спектра автокорреляционной функции имеют следующий вид:

. (3)

Традиционно, ценовые функции применяются для оптимизации отдельной булевой функции. Для всего же нелинейного узла замен cost функции, основанные на спектре Уолша-Адамара, можно обобщить следующим образом [6]:

(4)

и аналогично для cost функций, основанных на автокорреляционном спектре:

. (5)

Для оптимизации по критериям нелинейности и автокорреляции в [13] использовалась следующая функция стоимости:

(6)

В первой части проводимых в данной работе исследований использовались функции стоимости вида (3), (4), с заменой спектральных коэффициентов Уолша-Адамара и коэффициентов автокорреляционных спектров булевых функций на предложенные в [10] коэффициенты соответствующих спектров недвоичных функций.

Вторая часть проводимых исследований состояла в совершенствовании функций стоимости (критерия поиска криптографических функций), которое основывается на следующем положении. Известно, что при оптимизации криптографической функции по нелинейности и автокорреляции она по своим спектральным характеристикам (спектру корреляции с линейными функциями и автокорреляционному спектру) стремится к спектральным характеристикам бент-функций, что и было использовано в предыдущих работах [6, 13] при разработке функций вида (1)-(6). В тоже время, очевидным недостатком такого подхода является использование одного (фиксированного) значения статического коэффициента, к которому стремятся все спектральные значения оптимизируемой криптографической функции. При этом значения спектральных коэффициентов идеальной функции (или бент-функции) состоят из двух возможных значений для булевых функций, и из трех значений для введенных в [10] недвоичных функций. При введении же дополнительных ограничения на сбалансированность, количество возможных значений спектральных коэффициентов еще более возрастает.

При разработке новых функций стоимости предлагается в (2) - (6) заменить статический весовой коэффициент X на так называемые динамические весовые коэффициенты, т.е. весовые коэффициенты, принимающие различные значения для различных входных индексов спектра. В данной работе в качестве значений динамических весовых коэффициентов используются спектральные значения бент-функций. Предлагаемые функции стоимости имеют вид:

, (7), (8)

(9)

где $\hat{B}(\omega), r_B(s)$ – спектральные значения нелинейности и автокорреляции случайной недвоичной бент-функции B.

Таким образом, в основе предлагаемого вычислительного метода синтеза регулярных нелинейных узлов замен симметричных криптоалгоритмов лежит применение математического аппарата недвоичных криптографических функций [10], методов корреляционного и спектрального анализа, а также предложенных в данной работе усовершенствованных ценовых функций (7) – (9), с использованием динамических весовых коэффициентов $\hat{B}(\omega), r_B(s)$. Усовершенствованный таким образом метод имитации отжига позволяет, как показано ниже, реализовать вычислительный поиск регулярных узлов замен с требуемыми показателями нелинейности и автокорреляции.

Результаты экспериментальных исследований

Для подтверждения достоверности и обоснованности полученных теоретических результатов в данной работе проведены экспериментальные исследования эффективности предлагаемого вычислительного метода синтеза регулярных нелинейных узлов замен. Первая часть исследований была проведена с использованием спектров недвоичных функций со статическими весовыми коэффициентами в функциях стоимости (4) – (6) метода имитации отжига, вторая часть исследований – с использованием динамических коэффициентов $\widehat{B}(\omega), r_B(s)$ в функциях стоимости (7) – (9).

Параметры алгоритма для всех исследований были заданы следующими:

- α = 0.95 – параметр геометрического охлаждения;
- MIL = 500 – число шагов, предпринимаемых во внутреннем цикле;
- MaxIL = 300 – максимальное число внутренних циклов поиска;
- MUL = 50 – максимальное число последовательных непродуктивных внутренних циклов;
- количество пробегов алгоритма для каждого набора параметров равно 10.

В ходе экспериментов с функциями стоимости вида (4) – (6) использовались различные значения статических коэффициентов X и фиксированное значение R = 3.

Формировались S-блоки размерностей 8x2, 4x4, 6x4. Узлы замен выходной размерности 4 представлялись через одну недвоичную функцию над GF(2^4).

Полученные экспериментальные результаты для S-блоков 8x2 приведены в табл. 1. Лучший полученный результат выделен жирным шрифтом.

Таблица 1

Полученные результаты для S-блоков 8x2

Способ построения спектров	Статические коэффициенты		Динамические коэффициенты	
	NL	AC	NL	AC
WHT, ср.	110	56	114	24
WHT, худш.	108	56	**116**	**24**
ACT, ср.	110	48	114	24
ACT, худш.	112	40	114	24
WHT+ ACT, худш.	112	40	114	24
WHT+ ACT, ср.	112	40	114	24

Как видно из полученных результатов использование функций стоимости с динамическими весовыми коэффициентами позволило повысить показатели стойкости нелинейности и автокорреляции формируемых узлов замен.

В табл. 2 приведено сравнение полученных результатов с лучшими известными результатами, использующих традиционный подход описания S-блока в виде совокупности компонентных булевых функций [4-8]. Как видно из приведенной таблицы, полученные экспериментальные результаты предлагаемым методом с использованием функций стоимости на основе спектров недвоичных функций и статических весовых коэффициентов хорошо согласуются с экспериментальными результатами вычислительных методов традиционного подхода. Использование динамических весовых коэффициентов позволило получить лучшие известные на сегодняшний день результаты для S-блоков 8x2.

Таблица 2

Сравнение с результатами традиционного подхода, синтез S-блоков 8x2

Метод синтеза	NL	AC
Случайная генерация	108	56
Генетические алгоритмы	110	48
Имитация отжига (булевы функции)	114	32
Имитация отжига (недвоичные функции)	112	40
Имитация отжига (недвоичные функции, динамические весовые коэффициенты)	**116**	**24**

В табл. 3 приведены лучшие полученные результаты для S-блоков 4x4 и 6x4.

Таблица 3

Полученные результаты для S-блоков 4x4, 6x4

S-блок	Метод имитации отжига	NL	AC
4x4	Булевы функции	4	8
4x4	Функции над GF(2^4)	4	8
6x4	Булевы функции	22	24
6x4	Функции над GF(2^4)	**24**	**24**

Как видно из приведенной таблицы, применение предлагаемого подхода позволяет повысить нелинейность формируемых S-блоков 6x4.

Подобные S-блоки (размерности 6x4) применяются в DES-подобных шифрах.

Как показал проведенный анализ S-блоки DES по своим криптографическим показателям нелинейности NL и автокорреляции AC далеки от оптимальных (см. данные для S1-S8 в табл. 4). Разработанный вычислительный метод предлагается использовать для синтеза DES-подобных S-блоков с улучшенными криптографическими показателями стойкости (в табл. 4 приведены характеристики формируемых узлов замен S1*-S8*).

Таблица 4

Исследование криптографических свойств регулярных узлов замен 6x4

S-блок	NL	AC	DDT_{max}
S1	14	48	16
S2	16	56	16
S3	16	48	16
S4	16	64	16
S5	12	**40**	**16**
S6	**18**	48	16
S7	14	52	16
S8	16	48	16
S1*-S8*	**24**	**24**	**10**

Следует отметить, что для обеспечения стойкости DES-подобных шифров к дифференциальному и линейному криптоанализу сформированные S-блоки необходимо оценивать не только по показателям нелинейности и автокорреляции, но и с учетом других критериев, учитывающих саму структуру шифра [14]. В этом смысле оценка эффективности формируемых S-блоков с учетом ограничений, накладываемых особенностями основных преобразований БСШ, а также апробация полученных результатов являются перспективным направлением дальнейших исследований.

Выводы

Введенное теоретическое обобщение и предложенный математический аппарат недвоичных криптографических функций позволили усовершенствовать вычислительный метод формирования нелинейных узлов замен (метод имитации отжига). За счет сокращения количества оптимизационных спектров криптографических функций, описывающих S-блок, существенно ускоряется вычислительный поиск нелинейных узлов замен с требуемыми криптографическими свойствами.

Полученные результаты экспериментальных исследований эффективности предложенного метода вычислительного поиска с использованием ценовых функций стоимости и статическими весовыми коэффициентами согласуются с известными экспериментальными результатами для традиционного подхода. Использование предложенных в данной работе динамических весовых коэффициентов в предлагаемых функциях стоимости позволяют существенно повысить эффективность метода имитации отжига - получены лучшие известные на сегодняшний день результаты по нелинейности и автокорреляции для S-блоков 8x2. Для S-блоков 6x4 удалось поднять значение показателя нелинейности. Таким образом, разработанный вычислительный метод позволяет формировать нелинейные узлы замен с улучшенными свойствами и использовать их для совершенствования DES-подобных симметричных криптоалгоритмов.

Перспективным направлением дальнейших исследований является развитие математического аппарата криптографических недвоичных функций для задач синтеза биективных S-блоков, экспериментальные исследования эффективности предлагаемого подхода для узлов замен больших размерностей, обобщение введенных в данной работе динамических весовых коэффициентов.

Список литературы

1. *Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные коды на языке Си. – Триумф, 2002.*

2. *Burnett L. Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography // PhD thesis, Queensland University of Technology.*

3. *O'Connor L. An analysis of a class of algorithms for S-box construction // J. Cryptology,1994. – P. 133-151.*

4. *Millan W. How to improve the nonlinearity of bijective s-boxes // Information Security and Privacy, ACISP '98. - Springer Verlag, 1998. – volume 1438 of Lecture Notes in Computer Science. – P. 181-192.*

5. *Millan W., Burnett L., Carter G., Clark A., Dawson E. Evolutionary Heuristics for Finding Cryptographically Strong S-Boxes // Information and communication security. – Springer, Heidelberg, 1999. – Lecture Notes in Computer Science Volume 1726. – P.263-274.*

6. *Clark J.A., Jacob J.L., Stepney S. The Design of S-Boxes by Simulated Annealing // New Generation Computing. – 2005. – 23(3). – P.219–231.*

7. *Laskari C., Meletiou C., Vrahatis N. Utilizing Evolutionary Computation Methods for the Design of S-Boxes // Computational Intelligence and Security. – 2006. – Volume 2. – P.1299-1302.*

8. *Tesar P. A new method for generating high non-linearity S-Boxes // Radioengineering. – 2010. - Part 1 of II, Vol. 19 Issue 1. – P.23 -26.*

9. *Сорока Л.С., Кузнецов А.А., Исаев С.А. Исследование вероятностных методов формирования нелинейных узлов замен // Системи обробки інформації. – Х.:ХУВС, 2011. - № 8 (98).- С. 113 – 122.*

10. *Кузнецов А.А., Исаев С.А., Фролов В.В. Математическая модель регулярных нелинейных узлов замен с использованием недвоичных криптографических функций.*

11. *Dawson E., Millan W., Simpson L. Designing Boolean functions for cryptographic applications // Contributions to General Algebra. - Verlag Johannes Heyn, Klagenfurt, 2000. – 12. – P. 1-22.*

12. *Clark J.A., Jacob J.L., Stepney S., Maitra S., Milan W. Evolving Boolean functions satisfying multiple criteria // Lecture Notes in Computer Science (2551).- Springer , Berlin, 2002. - 2251. - P. 246-259.*

13. *Kavut S., Yücel M.D. Improved Cost Function in the Design of Boolean Functions Satisfying Multiple Criteria // Proc. INDOCRYPT. – 2003. – P..121-134.*

14. *Kwangjo K., Sangjin L., Sangjoon P., Daiki L. Securing DES S-Boxes against Three Robust Cryptanalysis // Proceedings of the Workshop on Selected Areas in Cryptography, SAC '95. – 1995. – P.145-157.*

Рецензент: д-р техн. наук, проф. Ю.В. Стасєв, Харківський університет Повітряних Сил імені. І. Кожедуба, Харків.

***Автор**: КУЗНЕЦОВ Александр Александрович*
Харьковский национальный университет им. В.Н. Каразина, Харьков, доктор технических наук, профессор, профессор кафедры безопасности информационных систем и технологий.
Раб. тел. - 057-752-64-15,
E-Mail –kuznetsov_alex@rambler.ru.

***Автор**: ИСАЕВ Сергей Александрович*
Харьковский национальный университет им. В.Н. Каразина, Харьков, аспирант кафедры безопасности информационных систем и технологий.
E-Mail – isaev.s23@gmail.com.

***Автор**: ФРОЛОВ Владислав Владимирович*
Харьковский национальный университет радиоэлектроники, Харьков, магистрант кафедры безопасности информационных технологий.
E-Mail – frolvlad@gmail.com.

УДК

Кузнецов О.О., Ісаєв С.О., Фролов В.В. Обчислювальний метод синтезу регулярних нелінійних вузлів замін з використанням недвійкових криптографічних функцій // Системи обробки інформації. – 2005. – Вип. 00 (00). – С. 00 – 00. – Рос.

Розглядаються обчислювальні методи синтезу регулярних нелінійних вузлів замін для симетричних криптографічних алгоритмів перетворення інформації. З використанням математичного апарату кореляційного та спектрального аналізу обґрунтовуються критерії пошуку недвійкових криптографічних функцій для нелінійних вузлів замін симетричних криптоалгоритмів. На основі удосконалених вагових коефіцієнтів цінових функцій пошуку пропонується подальший розвиток методу імітації відпалу (Simulated Annealing), досліджується ефективність пропонуємого підходу.

Табл. 4. Іл. 0. Бібліогр. 14 назв.

Кузнецов А.А., Исаев С.А., Фролов В.В. Вычислительный метод синтеза регулярных нелинейных узлов замен с использованием недвоичных криптографических функций // Системы обработки информации. - 2005. - Вып. 00 (00). - С. 00- 00 . - Рус.

Рассматриваются вычислительные методы синтеза регулярных нелинейных узлов замен для симметричных криптографических алгоритмов преобразования информации. С использованием математического аппарата корреляционного и спектрального анализа обосновываются критерии поиска недвоичных криптографических функций для нелинейных узлов замен симметричных криптоалгоритмов. На основе усовершенствованных весовых коэффициентов ценовых функций поиска предлагается дальнейшее развитие метода имитации отжига (Simulated Annealing), исследуется эффективность предлагаемого подхода.