**4.3. Совершенствование вычислительного метода синтеза регулярных нелинейных узлов замен**

Анализ открытой литературы показал, что на сегодняшний день существует целый ряд вычислительных методов синтеза регулярных нелинейных узлов замен, среди которых [66, 93‑94, 99‑100, 104]: 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 [66, 89] 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 [66].

Поиск начинается с некоторого начального состояния . Параметр T – некий контрольный параметр, известный как температура. Т инициализируется высокой температурой Т0 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, 𝛿 = 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; также – 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 n×m. 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 [66]:

.

Поскольку задача понижения автокорреляции представляется как задача минимизации максимального значения автокорреляционной функции, то cost функция в дальнейших исследованиях приняла следующий вид [66]:

.

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 [66]:



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

Известно, что равенство Парсеваля



ограничивает  значением равным как минимум 2n/2. Данная граница достигается тогда, когда выполняется равенство  для каждого w. 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

 (4.11)

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 [66] было введено обобщение функции стоимости (4.11), которое приняло следующий вид:

 . (4.12)

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 (4.12), функции стоимости относительно спектра автокорреляционной функции имеют следующий вид:

. (4.13)

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 [66]:

 (4.14)

и аналогично для cost функций, основанных на автокорреляционном спектре:

. (4.15)

Для оптимизации по критериям нелинейности и автокорреляции в [89] использовалась следующая функция стоимости:

 (4.16)

В первой части проводимых в данной работе исследований использовались функции стоимости вида (4.12), (4.13), с заменой спектральных коэффициентов Уолша-Адамара и коэффициентов автокорреляционных спектров булевых функций на предложенные выше 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 [66, 89] при разработке функций вида (4.11) – (4.16). 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 недвоичных функций. При введении же дополнительных ограничений на сбалансированность, количество возможных значений спектральных коэффициентов еще более возрастает.

При разработке новых функций стоимости предлагается в (4.12) – (4.16) 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:

, (4.17)

, (4.18)

 (4.19)

где – спектральные значения нелинейности и автокорреляции случайной недвоичной бент-функции B.

В целях нахождения наиболее эффективных критериев отбора криптографических недвоичных функций был проведен ряд исследований с использованием следующих функций стоимости. Используемые в классических критериях  и  для некоторой оптимизируемой булевой функции f(x) представляют собой разности числа совпадений в последовательностях функций f(x) и <w,x> (для нелинейности), f(xs) (для автокорреляции) и числа несовпадений, соответственно. В части исследований мы использовали в качестве функций стоимости число несовпадений (иными словами, расстояние Хэмминга) в таблицах истинности недвоичной функции F(X) и соответствующих последовательностях аффинных/линейных недвоичных функций (для исследования нелинейности), последовательностях F(X+S) (для исследования автокорреляции). Данный вид критериев в проводимых нами исследованиях был условно обозначен *«худшим» случаем*:

, (4.20)

, (4.21)

 (4.22)

, (4.23)

, (4.24)

(4.25)

Таким образом, в основе предлагаемого вычислительного метода синтеза регулярных нелинейных узлов замен симметричных криптоалгоритмов лежит применение математического аппарата недвоичных криптографических функций, методов корреляционного и спектрального анализа, а также предложенных в данной работе усовершенствованных ценовых функций (4.17) – (4.19) с использованием динамических весовых коэффициентов . Усовершенствованный таким образом метод имитации отжига позволяет реализовать вычислительный поиск регулярных узлов замен c требуемыми показателями нелинейности и автокорреляции.