Министерство образования и науки Украины

Исследование методов формирования нелинейных узлов замен блочных симметричных шифров

Выполнил
ст.гр. БИКСм-12-1
Фролов В.В.

Руководитель
д.т.н., проф. Кузнецов А.А.

Задачи

- Анализ методов формирования нелинейных узлов замен.
- Исследование и улучшение метода имитации отжига.
- Практические оценки повышения стойкости шифров (DES, MacGuffin, ГОСТ 28147-89) с использованием оптимальных S-блоков.
- Оценка производительности метода имитации отжига.

Классификация методов формирования нелинейных узлов замен

Методы случайной генерации	**Методы алгебраического построения**	**Методы эвристического поиска**
Случайная генерация с фильтрацией	Степенное отображение в поле	Метод имитации отжига
Побитовые методы	Инверсия в поле с афинными преобразованиями	Генетические алгоритмы

Метод имитации отжига

- Является универсальным оптимизационным алгоритмом.
- Представляет собой вероятностный вычислительный поиск оптимальных нелинейных узлов замен.
- Основывается на пошаговом улучшении S-блока за счёт постепенного снижения температурного показателя.
- Используется специальная ценовая функция.

Критерии отбора нелинейных узлов замен

- Нелинейность должна быть максимизирована.
- При равной нелинейности автокорреляция должна быть минимизирована.
- Дополнительные шифрозависимые критерии.

S-блоки шифра DES

- В DES используются S-блоки 6×4, $GF(2^6) \to GF(2^4)$
- К S-блокам DES выдвигается дополнительных 11 (8 основных и 3 дополнительных) критериев
- Метод имитации отжига формирует S-блоки с оптимальными показателями нелинейности ($NL = 24$) и автокорреляции ($AC = 24$)
- Метод имитации отжига не учитывает критерии DES

S-блоки шифра MacGuffin

- S-блоки 6×4, $GF(2^6) \to GF(2^2)$
- Нет дополнительных критериев, ограничивающих множество S-блоков

Сравнительный анализ исходных и оптимальных S-блоков MacGuffin

Криптографические показатели	**Исходные S-блоки**	**Оптимальные S-блоки**
Нелинейность (NL)	16 .. 20	24
Автокорреляция (AC)	32 .. 64	16
Δ-разность	32 .. 36	24
Лучшая линейная аппроксимация	12 .. 16	8

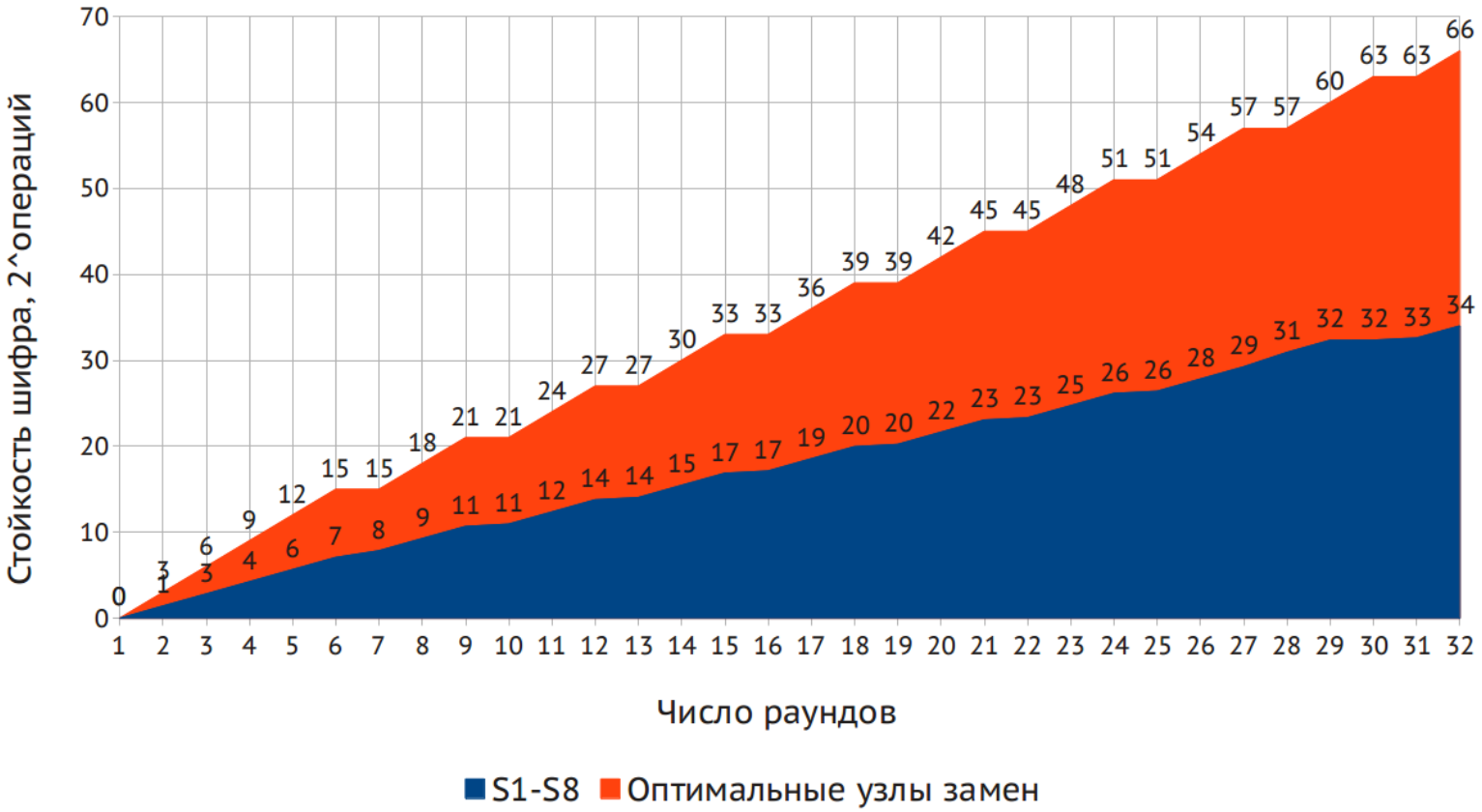
S-блоки шифра ГОСТ 28147-89

- Биективные S-блоки 4×4, $GF(2^4) \to GF(2^4)$
- Для оценки эффективности использовались оценки практической стойкости относительно верхней границы вероятности криптоанализа, полученные в работах Алексейчука и Ковальчука
- M_D — оценка вероятности дифференциального криптоанализа
- M_L — оценка вероятности линейного криптоанализа

Сравнительный анализ ЦБ РФ и оптимальных S-блоков ГОСТ 28147-89

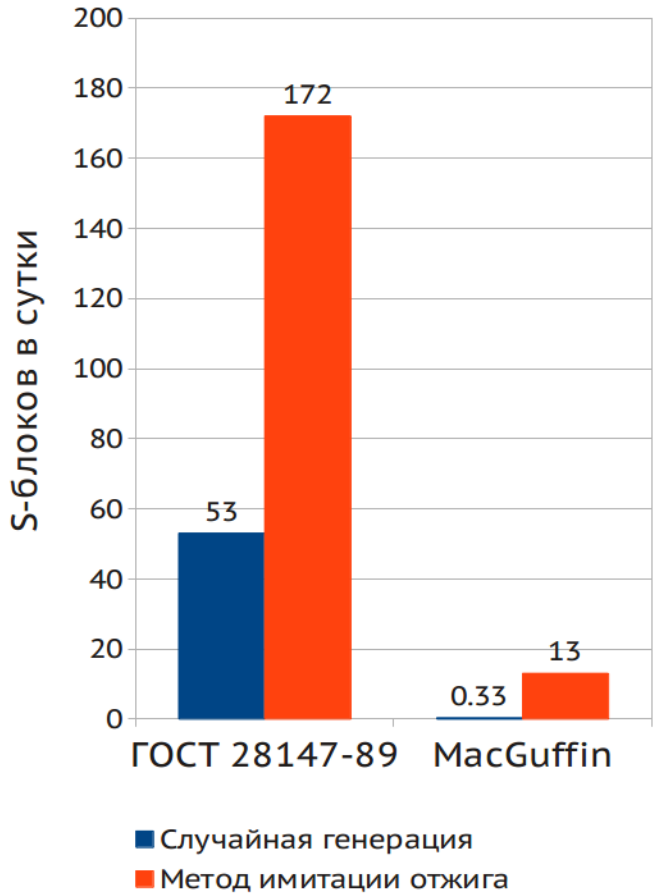
Криптографические показатели	**S-блоки ЦБ РФ**	**Оптимальные S-блоки**
Нелинейность (NL)	2 (лишь один S-блок имеет $NL = 4$)	4
Автокорреляция (AC)	16	8
M_D	$2^{-34.02}$	2^{-66}
M_L	$2^{-35.24}$	2^{-42}

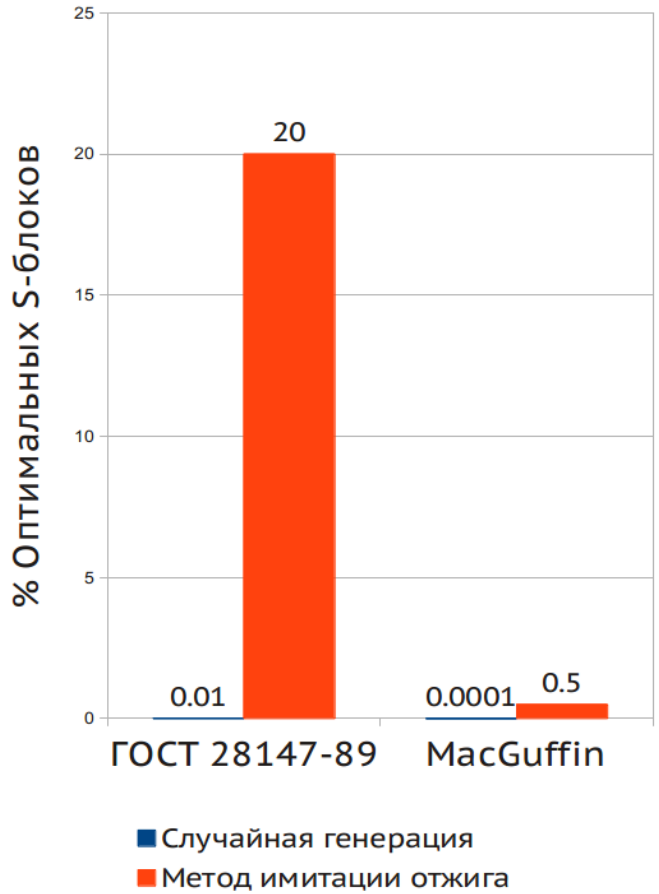
Эффективность ГОСТ 28147-89. Стойкость к дифференциальному криптоанализу



Эффективность ГОСТ 28147-89. Стойкость к линейному криптоанализу

Оценка поизводительности формирования S-блоков методом имитации отжига





Охрана труда и безопасность в чрезвычайных ситуациях

- Разработаны меры по охране труда в НИЛ с углублённой обработкой вопроса расчёта необходимой площади световых проёмов в помещении НИЛ.
- Суммарная расчётная площадь световых проёмов составляет 4,3 м^2, в то время как практическая площадь составляет 8 м^2.

Выводы

- Исследован и улучшен метод имитации отжига.
- Получены наглядные экпериментальные результаты повышения эффективности шифрования при использовании оптимальных S-блоков, сформированных методом имитации отжига.
- Оценена производительность метода имитации отжига относительно метода случайной генерации.

Спасибо за внимание.