

Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение   
высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

Институт искусственного интеллекта   
Базовая кафедра №252 – информационной безопасности

**курсовая работа по предмету**

**«КРИПТОГрафические методы защиты информации»**

**Тема работы:** Криптоанализ алгоритма симметричного шифрования SM4

|  |  |  |
| --- | --- | --- |
| **Студент группы ККСО-01-20** |  | *Семин В.В.* |
| **Руководитель** |  | *Старший преподаватель*  *Хомутов Дмитрий*  *Геннадьевич* |

ОГЛАВЛЕНИЕ

**Элементы оглавления не найдены.**

# 1 ОПИСАНИЕ АЛГОРИТМА

Описание алгоритма представлено в стандарте [1]. Алгоритм имеет размер блока 128 бит и размер ключа 128 бит. Его структура – несбалансированная сеть Фейстеля (за каждый раунд преобразуется 32 бита блока) с 32 раундами.

## 1.1 РАУНДОВАЯ ФУНКЦИЯ

Раундовая функция имеет вид (1.1).

|  |  |
| --- | --- |
|  | (1.1) |

Здесь – блок открытого текста, – раундовый ключ, – подстановка.

Подстановка является суперпозицией подстановки линейной подстановки и нелинейной подстановки , то есть .

В свою очередь имеет вид (1.2), а имеет вид (1.3).

|  |  |
| --- | --- |
|  | (1.2) |
|  | (1.3) |
| Результатом является блок зашифрованного текста |  |

## 1.2 РАСШИРЕНИЕ КЛЮЧА

Расширение ключа происходит по формуле (1.4)

|  |  |
| --- | --- |
|  | (1.4) |

Здесь , где – ключ, – константы; – константы; - подстановка, идентичная подстановке за исключением того, что вместо используется , имеющая формулу (1.5).

|  |  |
| --- | --- |
|  | (1.5) |

# 2 АТАКИ НА АЛГОРИТМ

## 2.1 ЛИНЕЙНАЯ АТАКА НА 22 РАУДОВЫЙ SM4

Статья [2] предлагает линейную атаку на 22 раундовый SM4. Для этого сначала строится линейная аппроксимация раундов 2-19, описанная уравнениями (2.1) – (2.6).

|  |  |
| --- | --- |
| ; раунд 5 | (2.1) |
| ; раунд 6 | (2.2) |
| ; раунд 10 | (2.3) |
| ; раунд 11 | (2.4) |
| ; раунд 15 | (2.5) |
| ; раунд 16 | (2.6) |

Здесь С учётом того, что равно :

|  |  |
| --- | --- |
| ; раунд 5 | (2.7) |
| ; раунд 6 | (2.8) |
| ; раунд 10 | (2.9) |
| ; раунд 11 | (2.10) |
| ; раунд 15 | (2.11) |
| ; раунд 16 | (2.12) |

Сложив уравнения (2.7) – (2.12), получим уравнение линейной аппроксимации раундов 2-19 (2.13).

|  |  |
| --- | --- |
|  | (2.13) |

Автор утверждает, что данная аппроксимация имеет отклонение .

Далее левая часть преобразуется для расширения на 22 раунда:

|  |  |
| --- | --- |
|  | (2.14) |

Здесь – правая часть уравнения (2.13), – результат шифрования 22 раундовым алгоритмом.

Выражение (2.14) имеет форму (2.15)

|  |  |
| --- | --- |
|  | (2.15) |

– функция чётности выражения, зависящая от открытого текста и закрытого. – функция, являющаяся композицией нескольких функций .

Так как в данной атаке количество активных s-боксов 6 для раундов 1, 20 и 8 для 21,22, то зависит 112 битного вектора , где , , , . Соответственно, представляется формулой (2.16).

|  |  |
| --- | --- |
|  | (2.16) |

Алгоритм атаки следующий:

1. Инициализировать вектор из элементов, каждый из которых соответствует возможному значению битов текста.
2. Для каждой пары векторов , вычислить чётность (чётность равна 1, если равно 0, -1 иначе). Сохранить результат в матрице , то есть
3. Вычислить чётность для каждого и прибавить её к соответствующему элементу .
4. Вычислить отклонение .
5. Если , то выбрать соответствующий вариант ключа и предположить

Если , то выбрать соответствующий вариант ключа и предположить

1. После получения значений остаётся перебрать 15 бит для получения ключа.

# 3 ПРАКТИЧЕСКАЯ ЧАСТЬ

## 3.1 ПРОВЕРКА ЛИНЕЙНОЙ АТАКА НА 22 РАУДОВЫЙ SM4

Проверка данного алгоритма была начата с проверки правдивости перехода от уравнения (2.13) к уравнению (2.14). Действительно, переход оказался верным:

.

# СПИСОК ЛИТЕРАТУРЫ

1. GMT 0002-2012 SM4分组密码算法 [Электронный ресурс]. Режим доступа: <https://github.com/guanzhi/GM-Standards/blob/master/GMT%E5%AF%86%E7%A0%81%E8%A1%8C%E6%A0%87/GMT%200002-2012%20SM4%E5%88%86%E7%BB%84%E5%AF%86%E7%A0%81%E7%AE%97%E6%B3%95.pdf> (Дата доступа 14.03.24).
2. Taehyun Kim, Jongsung Kim, Seokhie Hong, Jaechul Sung. Linear and Differential Cryptanalysis of Reduced SMS4 Block Cipher [Электронный ресурс]. Режим доступа: https://eprint.iacr.org/2008/281.pdf (Дата доступа 14.03.24).