СЛОЖЕНИЕ ПО МОДУЛЮ 2^n В БЛОЧНОМ ШИФРОВАНИИ

***Козлов Александр Александрович**, г. Москва*
***Карондеев Андрей Михайлович**, г. Москва*
***Силков Александр Андреевич**, г. Москва*

Работа посвящена анализу стойкости алгоритмов блочного шифрования, в которых операция смешения с ключом реализована как операция сложения по модулю 2^n. В ходе работы был произведен анализ криптографических свойств операции сложения по модулю 2^n. Предложены линейные и нелинейные аппроксимации данной операции, а также изучены особенности их использования при проведении криптоанализа. Приведен пример использования аппроксимаций сложения по модулю 2^n для проведения атаки типа Known Plaintext Attack на шифр, имеющий структуру SP–сети. Описанная в работе атака позволяет восстановить ключ быстрее полного перебора, что было подтверждено моделированием на ЭВМ. Показано, что замена операции побитового исключающего или (XOR) на сложение по модулю 2^n приводит к увеличению стойкости блочных шифров.

***Ключевые слова**: блочное шифрование (block cipher), сложение по модулю 2 (addition modulo 2^n)^n, линейный криптоанализ (linear cryptanalysis), нелинейный криптоанализ (nonlinear cryptanalysis).*

ADDITION MODULO 2^n IN BLOCK CIPHERS

***Aleksander Kozlov**, Moscow*
***Andrey Karondeev**, Moscow*
***Aleksander Silkov**, Moscow*

The article is devoted to the analysis of the resistance of block cipher algorithm which uses addition modulo 2^n operation as a key mixing operation. Analysis of cryptographic properties of the addition modulo 2^n operation was carried out in the article. Authors propose linear and non–linear approximations and their usage in cryptanalysis. Authors give an example of usage of the approximations for Known Plaintext Attack on SP–network cipher. Described attack allows recovering the key faster than full key lookup, it was confirmed by computer simulation. It has been shown that replacement of exclusive or operation(XOR) on the addition modulo 2^n operation increases resistance of block ciphers.

***Keywords**: addition modulo 2^n, block cipher, cryptanalysis.*

Составной частью любого блочного шифра является процедура смешения с ключом. Обычно данная процедура представляет собой не что иное, как простой XOR промежуточного информационного блока с раундовым ключом (как в алгоритмах DES, AES и др.), однако ничто не мешает использовать любую другую операцию, например сложение по модуль 2^n (как в алгоритме ГОСТ 28147-89). С учетом современной элементной базы и структуры большинства блочных шифров замена операции XOR на сложение по модулю 2^n не приведет к существенному возрастанию сложности как программной, так и аппаратной реализации шифра. Целью данной работы является изучение криптографических свойств операции $+ \ mod\ 2^n$, а также, на примере SP-сетей, оценка сложности проведения линейного криптоанализа при использовании операции сложения по модулю 2^n.

1. Линейные статистические аналоги сложения по модулю 2^n

Рассмотрим сложение двух n-разрядных чисел $A+B=D \ mod\ 2^n$, где $A=(a_{n-1}, a_{n-2}, \ldots, a_0)$, $B=(b_{n-1}, b_{n-2}, \ldots, b_0)$, $D=(d_{n-1}, d_{n-2}, \ldots, d_0)$. Его можно рассматривать как отображение:

$$Add\colon \mathbb{Z}_2^{2n} \to \mathbb{Z}_2^n, \qquad (1)$$

Обозначим аргументы этого отображения через $E = (a_{n-1}, b_{n-1}, \ldots, a_0, b_0)$.

Схематическое изображение блока $\sum mod\ 2^n$ приведено на рисунке 1.

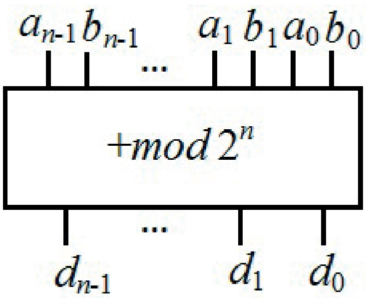

Рис. 1. Блок сложения по модулю $\mathbf{2^n}$

Рассмотрим координатные функции данного отображения. Их можно записать в виде:

$$d_i = a_i \oplus b_i \oplus p_i\,, \tag{2}$$

где p_i – значение переноса в i-й разряд, которое определяется следующим рекуррентным соотношением:

$$p_i = a_{i-1}b_{i-1} \vee a_{i-1}p_{i-1} \vee b_{i-1}p_{i-1},\ p_0 = 0, \tag{3}$$

Утверждение 1.

$$p_i(a_{i-1}, b_{i-1}, \dots, a_0, b_0) \notin aff\ , \forall i > 0, \tag{4}$$

где через *aff* обозначено множество аффинных функций.

Доказательство.

Преобразуем рекуррентное соотношение (3) $p_i = a_{i-1}b_{i-1} \oplus a_{i-1}p_{i-1} \oplus b_{i-1}p_{i-1}$, после чего становится видно, что АНФ, полученная развертыванием этого рекуррентного соотношения, содержит одночлены $a_{i-1}a_{i-2} \dots a_1 a_0 b_0$ и $b_{i-1}b_{i-2} \dots b_1 a_0 b_0$.

Как следствие, из равенства Парсеваля получаем соотношение:

$$\max_{\mathbf{u} \in \mathbb{Z}_2^{2i}} |W_{\hat{p}_i}(\boldsymbol{u})| < 2^{2i}, \tag{5}$$

где через $W_{\hat{f}}(\boldsymbol{u})$ обозначен $\boldsymbol{u}$-й коэффициент Уолша-Адамара.

Утверждение 2. Для любого $i > 0$ функция $p_i(a_{i-1}, b_{i-1}, \dots, a_0, b_0)$ не имеет фиктивных переменных.

Доказательство. В самом деле, переменная существенна тогда и только тогда, когда она входит в АНФ, а ранее при доказательстве утверждения 1 уже было показано, что АНФ функции p_i содержит одночлены $a_{i-1}a_{i-2} \dots a_1 a_0 b_0$ и $b_{i-1}b_{i-2} \dots b_1 a_0 b_0$.

Теорема 1.

Для любого $i > 0$ $\max_{\mathbf{u} \in \mathbb{Z}_2^{2i}} Prob\,(p_i = \langle \boldsymbol{u}, \boldsymbol{x} \rangle + c) \le 0.75$, причем равенство достигается на двух линейных функциях a_{i-1} и b_{i-1}.

Доказательство. Выразим вектор значений булевой функции p_i через вектор p_{i-1}:

Таблица 1.
Функция переноса $\boldsymbol{p_i}$

$a_{i-1}\ b_{i-1}\ a_{i-2}\ b_{i-2}\ \dots\ a_0\ b_0$	p_i
0 0 0 0 … 0 0	0
…	…
0 0 1 1 … 1 1	0
0 1 0 0 … 0 0	
…	p_{i-1}
0 1 1 1 … 1 1	
1 0 0 0 … 0 0	
…	p_{i-1}
1 0 1 1 … 1 1	
1 1 0 0 … 0 0	1
…	…
1 1 1 1 … 1 1	1

Если оба старших разряда слагаемых A и B равны нулю, переноса не происходит вне зависимости от значений остальных разрядов. Если же оба старших разряда равны единице, то перенос происходит всегда. В оставшихся случаях значение функции p_i совпадает со значением переноса из предыдущего разряда. Рассмотрим действительнозначный аналог функции $\hat{p}_i$ и вычислим преобразование Уолша-Адамара (преобразование Фурье 2 типа). Вычисления будем производить по схеме «бабочка». Последние две итерации приведены в таблице 2.

В связи с особенностями строения функции p_i, столбец значений поделен на четыре части. Вычисляя преобразование Уолша-Адамара по схеме «бабочка» на предпредпоследнем шаге имеем вычисленные вектора преобразовании от каждого из четырех блоков. Далее проделываем последние два шага.

Проанализируем результат. Из (5) следует, что значения элементов первого и четвертого блоков по модулю строго меньше 2^{2i-1}. Поэтому значение 2^{2i-1} является максимальным по модулю среди коэффициентов Уолша-Адамара функции p_i и достигается на двух аргументах (1000…00) и (0100…00). Эти наборы соответствуют линейным функциям a_{i-1} и b_{i-1}, а значение коэффициента Уолша-Адамара дает указанную вероятность совпадения 0.75.

Как следствие из теоремы 1 имеем:

Для любого i от 0 до n для i-го выхода $D = A + B \bmod 2^n$ справедливы соотношения:

Таблица 2.
Вычисление преобразования Уолша-Адамара от функции переноса $\boldsymbol{p_i}$

$a_{i-1}\ b_{i-1}\ \dots\ a_0\ b_0$	p_i	$\hat{p}_i$	$\dots$			$W_{\hat{p}_i}$
0 0 0 … 0 0 0 0 1 … 1 1	0 … 0	1 … 1		2^{2i-2} 0 … 0	$2^{2i-2}+W_{\hat{p}_{i-1}}(\mathbf{0})$ $W_{\hat{p}_{i-1}}$	$2W_{\hat{p}_{i-1}}$
0 1 0 … 0 0 0 1 1 … 1 1	p_{i-1}	$\hat{p}_{i-1}$		$W_{\hat{p}_{i-1}}$	$2^{2i-2}+W_{\hat{p}_{i-1}}(\mathbf{0})$ $-W_{\hat{p}_{i-1}}$	2^{2i-1} 0 … 0
1 0 0 … 0 0 1 0 1 … 1 1	p_{i-1}	$\hat{p}_{i-1}$		$W_{\hat{p}_{i-1}}$	$W_{\hat{p}_{i-1}}(\mathbf{0})-2^{2i-2}$ $W_{\hat{p}_{i-1}}$	2^{2i-1} 0 … 0
1 1 0 … 0 0 1 1 1 … 1 1	1 … 1	–1 … –1		-2^{2i-2} 0 … 0	$2^{2i-2}+W_{\hat{p}_{i-1}}(\mathbf{0})$ $W_{\hat{p}_{i-1}}$	$-2W_{\hat{p}_{i-1}}$

$$Prob(d_i = a_i \oplus b_i \oplus a_{i-1}) =$$

$$= Prob(d_i = a_i \oplus b_i \oplus b_{i-1}) = 0.75,$$

причем эти два статистических аналога функции d_i является наилучшими среди всех линейных.

Утверждение 3.

$$\forall i > 0 \quad W_{\hat{p}_i}(\mathbf{0}) = 2^i \ll 2^{2i}$$

Доказательство.

$a_0\ b_0$	$p_1 = a_0 b_0$		
0 0	0	1	2
0 1	0	1	2
1 0	0	1	2
1 1	1	-1	-2

В самом деле, для $i = 1$ утверждение верно, далее утверждение непосредственно следует из таблицы 2.

При проведении криптоанализа может быть полезна аппроксимация для суммы *mod 2* нескольких выходов. Докажем следующее утверждение о сумме *mod 2* для двух соседних выходов блока + *mod* 2^n

Утверждение 4.

$$Prob(d_i \oplus d_{i-1} = a_i \oplus b_i \oplus 1) = 0.75$$

Доказательство.

Для начала рассмотрим сумму переносов из соседних разрядов

Таблица 3.
Сумма mod 2 соседних разрядов переноса

a_{i-1}	b_{i-1}	$p_i \oplus p_{i-1}$
0	0	p_{i-1}
0	1	0
1	0	0
1	1	$p_{i-1} \oplus 1$

Из таблицы 3 видно, что $Prob(p_i \oplus p_{i-1} = a_{i-1} \oplus b_{i-1} \oplus 1) = 0.75$. Прибавим к обеим частям равенства величин $a_i \oplus b_i \oplus a_{i-1} \oplus b_{i-1}$ и тогда, с учетом (2), получаем искомое утверждение: $Prob(d_i \oplus d_{i-1} = a_i \oplus b_i \oplus 1) = 0.75$.

Стоит отметить, что рассмотренные ранее статистические соотношения справедливы, только если случайные величины $a_i, b_i, a_{i-1}, b_{i-1}, \dots, a_0, b_0$ независимы и принимают всевозможные значения с равной вероятностью.

2. Особенности использования линейных статистических аналогов при анализе блочных

шифров

Для примера рассмотрим один из классических блочных шифров, а именно SP-сеть с размером блока 16 бит и 4 раундами шифрования. Каждый цикл, кроме последнего, состоит из 3 операций (Рисунок 2):

- Смешение информационного блока с подключом
- Нелинейное преобразование, реализуемое слоем S-блоков
- Линейное преобразование, реализуемое P-блоком

В последнем раунде отсутствует P-блок и на выходе производится смешение с подключом (Рисунок 2). Ключ состоит из 80 бит, разбитых на 5 подключей по 16 бит каждый. В качестве операции смешения с подключом будем использовать сложение $mod\ 2^n$.

Все P-блоки описываются таблицей 4:

Все S-блоки описываются таблицей 5:

Обозначим, через $X_{i,j}$ – j-й бит входа в i-й блок смешения с подключом, через $Y_{i,j}$ – j-й бит выхода из i-того блока смешения с подключом, а через $V_{i,j}$– j-й бит выхода из i-го слоя S-box.

Будем считать, что нам известно достаточное количество пар открытый текст – шифртекст полученных на одном ключе, который необходимо восстановить.

Важной особенностью является то, что ключ фиксирован и операция смешения с подключом по сути представляет собой сложение с константой. Поэтому полученные ранее оценки для линейной аппроксимации сложения не работают, так как были получены из предположения, что оба слагаемых выбираются случайно равновероятно, а это условие не выполняется при фиксированном ключе. Более того справедливо следующие утверждения:

Утверждение 5.

Для любого $i > 0$ и любого фиксированного $k = (k_0, k_1, \dots, k_{i-1})$ $Prob(p_i = x_{i-1}) = \frac{1}{2} + \varepsilon$, где $0 \le |\varepsilon| \le 0.5$ причем обе границы достигаются на ключах $k = (0,0,\dots,0)$ и

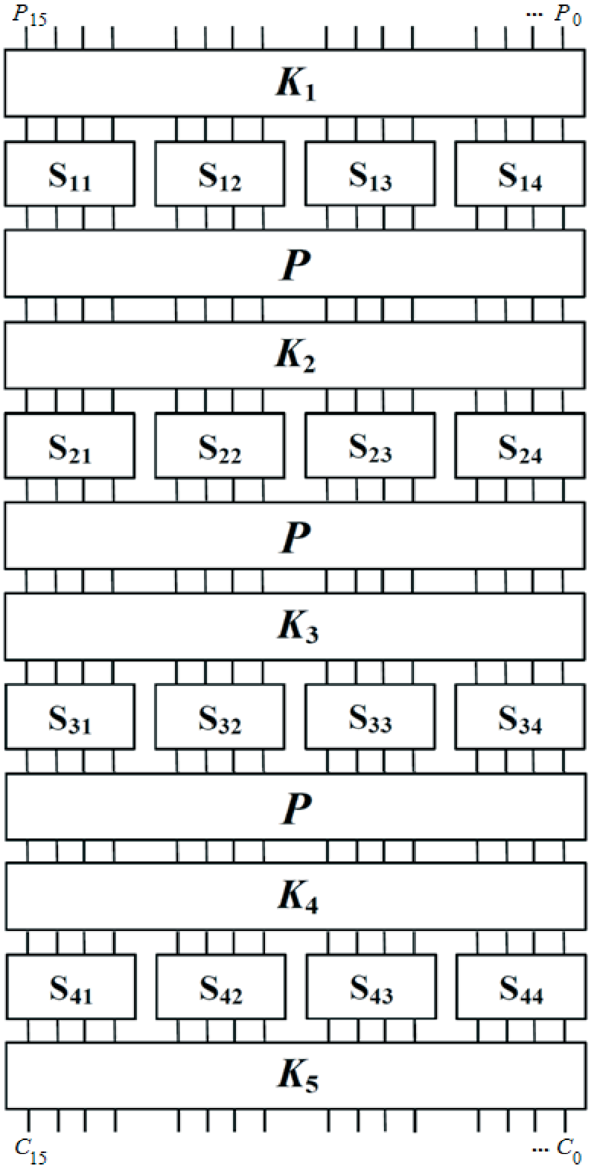

Рис. 2. *Схема шифрования*

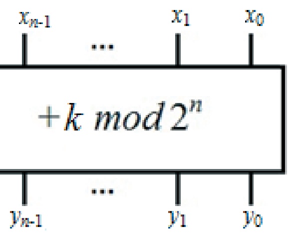

Рис. 3. *Блок смешения с подключом*

Таблица 4.
Описание P-блока

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15

Таблица 5.
Описание S-блока

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
9	0	12	4	6	2	10	8	3	11	15	5	7	14	1	13

$k = (0,0,\ldots,0,1)$ соответственно.

Доказательство.

При $k = (0,0,\ldots,0)$ перенос в i-й разряд никогда не происходит, а мы считаем, что он происходит при x_{i-1}=1. Так как функция x_{i-1} линейна и как следствие равновесна, при данной аппроксимации мы ошибемся в половине случаев.

При $k = (0,0,\ldots,0,1)$ перенос в (i-1)-й разряд никогда не происходит, а перенос в i-й разряд полностью определяется значением x_{i-1}.

Утверждение 6.

Для любого $i > 0$ и любого фиксированного $k = (k_0, k_1, \ldots, k_{i-1})$ $Prob(p_i = k_{i-1}) = \frac{1}{2} + \varepsilon$, где $0 \leq |\varepsilon| \leq 0.5$ причем обе границы достигаются на ключах $k = (0,0,\ldots,0,1)$ и $k = (0,0,\ldots,0)$ соответственно.

Доказательство.

При $k = (0,0,\ldots,0,1)$ перенос в (i-1)-й разряд никогда не происходит, а перенос в i-й разряд полностью определяется значением x_{i-1}, а мы считаем, что он есть всегда. Так как функция x_{i-1} линейна и как следствие равновесна, при данной аппроксимации мы ошибемся в половине случаев.

При $k = (0,0,\ldots,0)$ перенос в i-й разряд никогда не происходит, как мы и предполагаем.

Утверждения 5, 6 можно усилить, а именно при изменении $k = (k_{i-1}, k_{i-2}, \ldots, k_0)$ от $(0,0,\ldots,0)$ до $(1,0,\ldots,0)$ $Prob(p_i = x_{i-1})$ монотонно возрастает от 0.5 до 1, а $Prob(p_i = k_{i-1})$ монотонно убывает от 1 до 0.5, а также при изменении $k = (k_{i-1}, k_{i-2}, \ldots, k_0)$ от $(1,0,\ldots,0)$ до $(1,1,\ldots,1)$ $Prob(p_i = x_{i-1})$ монотонно убывает от 1 до 0.5, а $Prob(p_i = k_{i-1})$ монотонно возрастает от 0.5 до 1 (Рисунок 4). Последнее легко доказывается сопоставлением случаев, когда действительно происходит перенос, с функциями x_{i-1} и k_{i-1} соответственно.

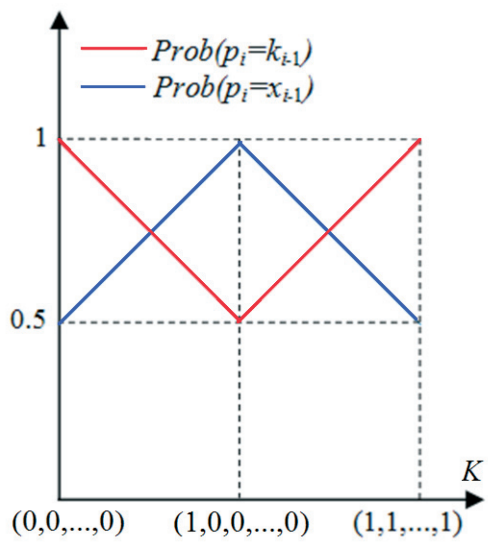

Рис. 4. *Значения $Prob(p_i=k_{i-1})$ и $Prob(p_i=x_{i-1})$ на различных k*

Учитывая то, что на фиксированном заранее не известном ключе рассмотренные ранее соотношения в худшем случаи, будут выполняться с вероятностью 0.5 ($bias$=0) из чего следует, что они не применимы для проведения линейного криптоанализа в чистом виде. Однако учитывая тот факт, что наихудший случай соответствует ключу специального вида, а также монотонность изменения вероятности выполнения аппроксимации при изменении ключа, в случаи возникновения неуспеха при проведении линейного криптоанализа с использованием данных соотношений можно получить некую информацию о ключе.

3. Нелинейные статистические аналоги сложения по модулю 2^n

Пусть $X+K=Y \bmod 2^n$, где $X=(x_{n-1}, x_{n-2}, \ldots, x_0)$, $Y=(y_{n-1}, y_{n-2}, \ldots, y_0)$, а $K=(k_{n-1}, k_{n-2}, \ldots, k_0)$=const.

Лемма 1. Для любого фиксированного K, найдется z такое, что

$$\forall i > 0 \ Prob(y_i = x_i \oplus z \cdot x_{i-1}) = \frac{1}{2} + \varepsilon, \quad (7)$$

где $|\varepsilon| \geq \frac{1}{4}$

Доказательство. Зафиксируем k_i и k_{i-1}.

При $k_i = 0$, $k_{i-1} = 0$

x_i	x_{i-1}	y_i	$x_i \oplus z \cdot x_{i-1}$
0	0	0	0
0	1	p_{i-1}	z
1	0	1	1
1	1	$1 \oplus p_{i-1}$	$1 \oplus z$

Если $Prob(p_{i-1}=0)>0.5$, положим $z=0$, иначе $z=1$.

При $k_i = 0$, $k_{i-1} = 1$

x_i	x_{i-1}	y_i	$x_{i-1} \oplus z \cdot x_{i-1}$
0	0	p_{i-1}	0
0	1	1	z
1	0	$1 \oplus p_{i-1}$	1
1	1	0	$1 \oplus z$

Если $Prob(p_{i-1}=0)>0.5$, положим $z=1$, иначе $z=0$.

При $k_i = 1$, $k_{i-1} = 0$

x_i	x_{i-1}	y_i	$x_{i-1} \oplus z \cdot x_{i-1}$
0	0	1	0
0	1	$1 \oplus p_{i-1}$	z
1	0	0	1
1	1	p_{i-1}	$1 \oplus z$

Если $Prob(p_{i-1}=0)>0.5$, положим $z=0$, иначе $z=1$.

При $k_i=1, k_{i-1}=1$

x_i x_{i-1}	y_i	$x_{i-1}\oplus z\cdot x_{i-1}$
0 0	$1\oplus p_{i-1}$	0
0 1	0	z
1 0	p_{i-1}	1
1 1	1	$1\oplus z$

Если $Prob(p_{i-1}=0)>0.5$, положим $z=1$, иначе $z=0$.

Лемма 2. Для любого фиксированного K, найдется z такое, что

$$\forall i > 0 \;\; Prob(y_i \oplus y_{i-1} = x_i \oplus z \cdot x_{i-1}) = \frac{1}{2} + \varepsilon,$$

где $|\varepsilon| \geq \frac{1}{4}$ (8)

Доказательство. Зафиксируем k_i и k_{i-1}.

При $k_i=0, k_{i-1}=0$

x_i x_{i-1}	$y_i\oplus y_{i-1}$	$x_i\oplus z\cdot x_{i-1}$
0 0	p_{i-1}	0
0 1	1	z
1 0	$1\oplus p_{i-1}$	1
1 1	0	$1\oplus z$

Если $Prob(p_{i-1}=0)>0.5$, положим $z=1$, иначе $z=0$.

При $k_i=0, k_{i-1}=1$

x_i x_{i-1}	$y_i\oplus y_{i-1}$	$x_{i-1}\oplus z\cdot x_{i-1}$
0 0	1	0
0 1	$1\oplus p_{i-1}$	z
1 0	0	1
1 1	p_{i-1}	$1\oplus z$

Если $Prob(p_{i-1}=0)>0.5$, положим $z=0$, иначе $z=1$.

При $k_i=1, k_{i-1}=0$

x_i x_{i-1}	$y_i\oplus y_{i-1}$	$x_{i-1}\oplus z\cdot x_{i-1}$
0 0	$1\oplus p_{i-1}$	0
0 1	0	z
1 0	p_{i-1}	1
1 1	1	$1\oplus z$

Если $Prob(p_{i-1}=0)>0.5$, положим $z=1$, иначе $z=0$.

При $k_i=1, k_{i-1}=1$

x_i x_{i-1}	$y_i\oplus y_{i-1}$	$x_{i-1}\oplus z\cdot x_{i-1}$
0 0	0	0
0 1	p_{i-1}	z
1 0	1	1
1 1	$1\oplus p_{i-1}$	$1\oplus z$

Если $Prob(p_{i-1}=0)>0.5$, положим $z=0$, иначе $z=1$.

Соотношения, рассмотренные в леммах 1, 2, в отличие от рассмотренных линейных статистических аналогов, выполняются с преобладанием существенно больше нуля для всех ключей K, соответственно их использование повышает эффективность при проведении криптоанализа.

4. Криптоанализ на основе нелинейных статистических аналогов

4.1. Описание метода криптоанализа

Общая идея – получить соотношение связывающие некоторые биты открытого текста, шифртекста и ключа, которое выполняется с преобладанием (*bias*) существенно больше нуля. Соотношения (7) и (8) не являются линейными. Покажем, что это не мешает использовать лемму о накапливании. Действительно как было показано в леммах 1, 2 для фиксированного ключа, наибольшее преобладание достигается при фиксированном z. После подстановки этого z, нелинейных членов не остается и мы получаем линейное соотношение, для которого применима лемма о накапливании. Заранее не известно при каком z преобладание будет максимальным, но известно что среди всех значений будет такое z для которого мы гарантировано получим высокое преобладание, поэтому будем перебирать всевозможные z. По сути, каждому z соответствует конкретное линейное соотношение. Итого получаем несколько линейных соотношений, одно из которых гарантированно выполняется с большим значением преобладания.

С учетом вышесказанного произведем криптоанализ блочного шифра описанного в 3 части, более детальная схема которого изображена на рисунке 5.

5.1. Используемые аппроксимации

Для проведения анализа будем использовать следующие соотношения:

1. Нелинейные соотношения для блока сложения по модулю 2^n:

- $\exists z$: $x_i \oplus x_{i-1} z = y_i$ выполняется с преобладанием больше $\frac{1}{4}$
- $\exists z$: $x_i \oplus x_{i-1} z = y_i \oplus y_{i-1}$ выполняется с преобладанием больше $\frac{1}{4}$

2. Корреляционную матрицу S-блока

Корреляционная матрица рассматриваемого S-блока приведена на таблице 6 (выделенные

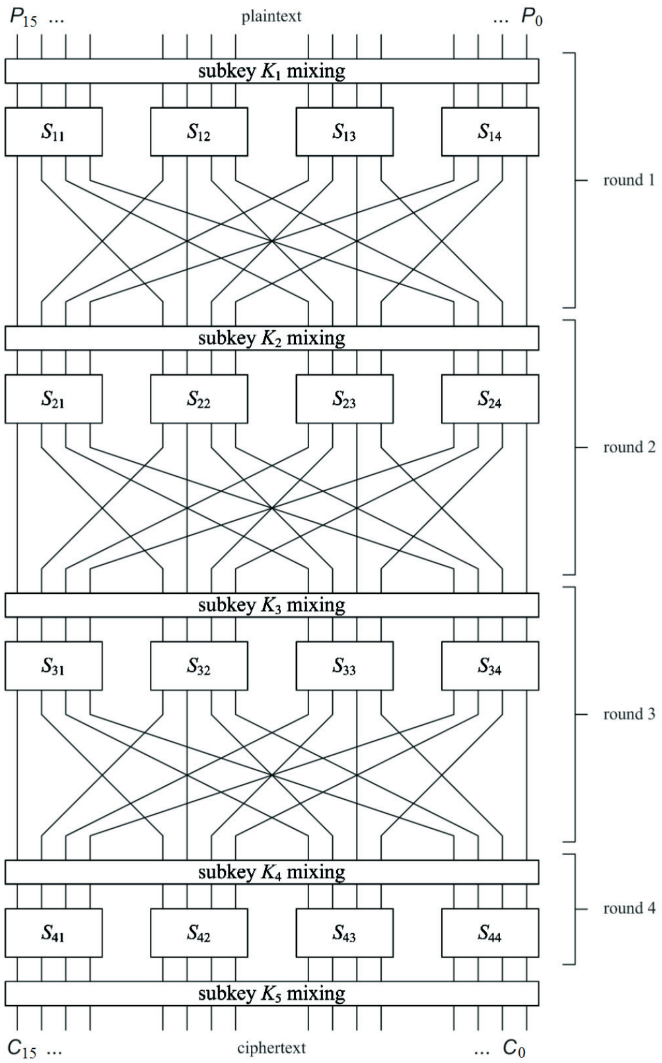

Рис. 5. *Схема шифрования*

ячейки соответствуют аппроксимациям, используемым в активных S-блоках).

Активными назовем S-блоки, лежащие на пути аппроксимации. Активные блоки выбирались так, чтобы максимизировать преобладание конечного соотношения. При построении пути, при аппроксимации блока сложения два соседних входных разряда переходят в соответствующие два выходных разряда или только в старший. Поэтому необходимо строить путь, покрывающий соседние разряды, что сильно усложняет процесс построения пути.

На рисунке 6 приведен путь используемой аппроксимации:

Согласно приведенной схеме активными S-блоками являются:

$S_{1,1}, S_{2,1}, S_{2,2}, S_{3,4}$

Для каждого из них выполняются следующие линейные соотношения:

- $S_{11}: V_2 = Y_1 \oplus Y_2$, выполняется с $bias = \frac{3}{8}$
- $S_{21}: V_0 = Y_0$, выполняется с $bias = \frac{1}{8}$
- $S_{22}: V_0 = Y_3$, выполняется с $bias = \frac{3}{8}$
- $S_{34}: V_0 = Y_3$, выполняется с $bias = \frac{3}{8}$

Для каждого из блоков сложения используем следующие соотношения:

- $\exists z_0: X_{1,14} \oplus X_{1,13} z_0 = Y_{1,14} \oplus Y_{1,13}$, выполняется с $bias \geq \frac{1}{4}$
- $\exists z_1: X_{2,12} \oplus X_{2,11} z_1 = Y_{2,12} \oplus Y_{2,11}$, выполняется с $bias \geq \frac{1}{4}$
- $\exists z_2: X_{3,3} \oplus X_{3,2} z_2 = Y_{3,3}$, выполняется с $bias \geq \frac{1}{4}$
- $\exists z_3: X_{2,12} \oplus X_{2,11} z_3 = Y_{2,12}$, выполняется с $bias \geq \frac{1}{4}$
- $X_{4,0} = Y_{4,0}$, выполняется с $bias \geq \frac{1}{4}$

Итоговое соотношение имеют вид:

$$V_{1,3} \oplus z_1 (P_{14} \oplus z_0 P_{13}) = Y_{4,0} \quad (9)$$

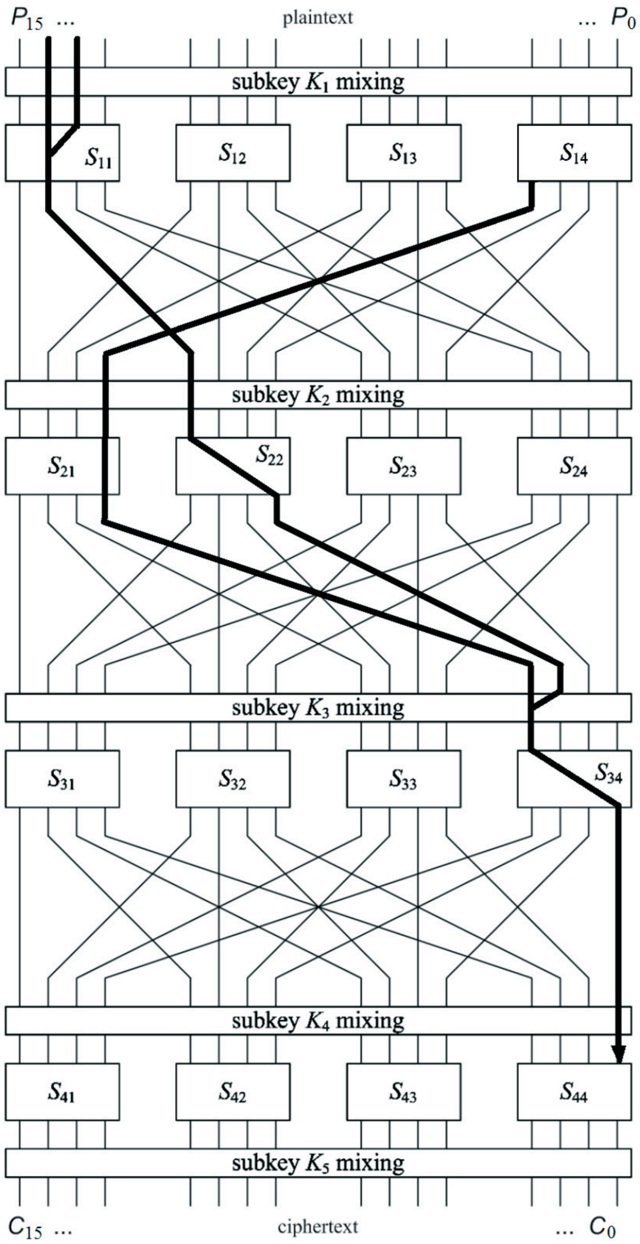

Рис. 6. *Схема нелинейной аппроксимации*

Значение $V_{1,3}$ получаем из открытого текста и перебираемой части первого подключа, а $Y_{4,0}$ из шифртекста и перебираемой части пятого подключа, обращения часть схемы. Согласно лемме о накапливании, для соотношения (9) найдутся такие z_i, что на истинном ключе оно будет выполняется с преобладанием больше чем $2^6 \cdot (\frac{1}{4})^3 \cdot (\frac{3}{8})^3 \cdot \frac{1}{8} = \frac{27}{4096}$ соответственно для проведения криптоанализа в худшем случаи будет достаточно иметь порядка 23 тысяч пар открытый текст – шифртекст. Для проведения анализа необходимо перебрать 4 младших бита первого и пятого подключей, а также значения $z_i(2^{4+4+2} = 2^{10})$. Моделирование на ЭВМ показало, что в среднем достаточно порядка 5 тысяч пар открытый текст - шифртекст.

Ход криптоанализа:

1. Для восстанавливаемого ключа сгенерировать 23000 случайных пар открытый текст – шифртекст

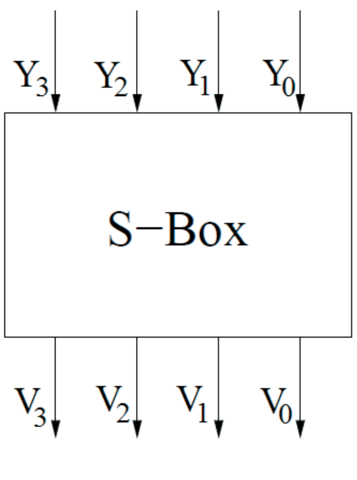

Рис. 7. *Схема S-блока*

Таблица 6.
Корреляционная матрица S-блока

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0001	0	-4	0	-4	-4	0	-4	0	12	0	-4	0	0	-4	0	-4
0010	0	-4	-8	4	4	0	4	-8	0	-8	-8	0	0	0	0	0
0011	0	0	0	0	8	0	0	-8	0	-8	-8	0	0	0	0	0
0100	0	0	4	-4	0	0	12	4	4	-4	0	0	-4	4	0	0
0101	0	-4	-4	0	-4	0	0	-4	0	-4	4	-8	-4	0	8	4
0110	0	4	4	0	-4	0	0	-4	0	-4	4	8	4	0	8	-4
0111	0	-8	4	4	0	0	4	-4	-4	4	0	0	-4	-4	0	-8
1000	0	0	4	4	0	-8	-4	4	0	-8	4	-4	0	0	-4	-4
1001	0	-4	4	0	4	0	0	-4	4	0	8	4	0	-4	-4	8
1010	0	-4	-4	-8	4	-8	0	4	-4	0	0	4	0	-4	4	0
1011	0	0	4	4	0	0	4	4	0	0	-4	-4	8	-8	4	4
1100	0	0	0	-8	0	8	0	0	-4	-4	4	-4	4	-4	-4	-4
1101	0	-4	8	-8	4	0	-4	0	0	4	0	-4	4	8	4	0
1110	0	4	0	-4	-4	-8	4	-8	0	4	0	-4	4	0	-4	0
1111	0	8	0	0	8	0	0	0	4	4	4	-4	-4	-4	4	-4

2. Для сгенерированных пар и всевозможных значений части ключа $K_{1,0}, K_{1,1}, K_{1,2}, K_{1,3}, K_{5,0}, K_{5,1}, K_{5,2}, K_{5,3}$ и параметров z_0, z_1 вычислить преобладание, с которым выполняется соотношение 9
3. Значения части ключа, на котором соотношение 9 выполняется с наибольшим преобладанием принимаем за истинные.
4. Оставшиеся биты находим тотальным опробованием

6. Выводы

Проведенный выше анализ использования сложения по модулю 2^n в блочном шифровании показывает:

- Замена блока смешения с ключом со сложения по модулю 2 на сложение по модулю 2^n существенно осложняет линейный криптоанализ.
- Существуют алгоритмы взлома такого шифра быстрее полного перебора, при этом наилучшие результаты дает использование нелинейных аппроксимаций.
- При проведении криптоанализа возможно комбинирование описанных методов. Сначала необходимо воспользоваться методом линейных аппроксимаций, а при неудачном исходе использовать нелинейные методы.

Литература (References)

1. Mukhopadhyay D., Design and Analysis of Cellular Automata Based Cryptographic Algorithms. Ph.D. thesis, Indian Institute of Technology, Kharagpur, 2007
2. Matsui M., Linear Cryptanalysis Method for DES Cipher. In Advances in Cryptology—Proceedings of EUROCRYPT '93, LNCS v. 765, pp. 386 – 397, Springer, 1994
3. Li An-Ping, Linear Approximating to Integer Addition. https://eprint.iacr.org/2006/457.pdf
4. Wallen J., Linear Approximations of Addition Modulo 2n. Fast Software Encryption — FSE'2003, LNCS v. 288, pp. 261 – 273, Springer-Verlag, 2003.