электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 02, февраль 2016

УДК 004.056

Криптографический анализ ARX шифров на основе усеченных разностей

***Козлов А.А.**, специалист*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Жуков А.Е., к.ф-м.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра Информационная безопасность»
iu8@bmstu.net

1. Введение

Многие криптографические алгоритмы создаются, используя операции сложения по модулю 2^n, циклического сдвига, и сложения по модулю 2 (*XOR*). Криптографические алгоритмы, использующие только эти операции, называются *ARX* алгоритмами шифрования. Преимуществом использования этих операций является то, что они очень быстры при программной реализации. В то же время при их правильной композиции, они обладают хорошими криптографическими свойствами. Сложение по модулю 2^n вносит нелинейность, циклический сдвиг обеспечивает рассеивание в пределах одного слова, а *XOR* вносит рассеивание между словами. Недостатком использования подобных операций является тот факт, что рассеивание происходит, как правило, медленно. Это часто компенсируется большим числом раундов в криптографических алгоритмах.

Примером криптографических алгоритмов, использующих сложение по модулю 2^n, циклический сдвиг и *XOR*, для поточных шифров являются шифры *Salsa20* и *HC-128*, для блочных шифров это *TEA*, *XTEA*, *FEAL*, *Threefish* , а так *Speck*.

На текущий момент существующие работы по исследованию криптографической стойкости ARX шифров, использующие в качестве метода криптографического анализа метод разностного анализа, показывают, что классический разностный анализ невозможно провести для полного числа раундов любого современного *ARX* шифра.

В настоящей работе предложен новый подход к оценке разностных свойств операции сложения по модулю 2^n. На основании этого подхода был определен класс *ARX* шифров, подверженный атаке с использованием усеченных разностей операции сложения

по модулю 2^n.

2. Усеченные разности сложения по модулю 2^n

В ряде случаев, когда невозможно построить разностную характеристику с достаточно высокой вероятностью, возможно найти такую разностную характеристику, которая использует не целиком разность между двумя открытыми текстами, а некие усеченные разности (truncated differentials) – разность между определенными подблоками обрабатываемых данных. При этом, вероятность таких характеристик может быть существенно выше, чем вероятность классических «полных» характеристик.

Обозначим через xdp^+ вероятность распространения разности по модулю 2 через операцию сложения по модулю 2^n. Рассмотрим вычисление xdp^+ для двух n-битных разностей. Пусть нам заданы входные разности A и B, $A=(a_{n-1},a_{n-2},...,a_0)$, $B=(b_{n-1},b_{n-2},...,b_0)$ и выходная разность Q, $Q=(q_{n-1},q_{n-2},...,q_0)$ для операции сложения по модулю 2^n, с операцией сложения по модулю 2 в качестве операции разности. Обозначим через A_{i-1}, B_{i-1} и Q_{i-1} первые $i-1$ бит разностей A, B, и Q, $A_{i-1}=(a_{i-1},a_{n-2},...,a_0)$, $B_{i-1}=(b_{i-1},b_{n-2},...,b_0)$, $Q_{i-1}=(q_{i-1},q_{n-2},...,q_0)$. Через $\Pr ob_{Q_{i-1}}=C$ — обозначим $xdp^+(A_{i-1},B_{i-1}\to Q_{i-1})$. Тогда для битов a_i, b_i и q_i справедлива следующая теорема.

Теорема 1. Для заданных входных разностей A и B, и выходной разности Q, для операции сложения по модулю 2^n, с операцией *XOR* в качестве операции разности, если известно, что $xdp^+(A_{i-1},B_{i-1}\to Q_{i-1}) = \Pr ob_{Q_{i-1}}$, то:

если $a_{i-1}=b_{i-1}=q_{i-1}=0$, то $\Pr ob_{Q_i^*}=\Pr ob_{Q_{i-1}}$, $\Pr ob_{Q_i^1}=0$,

если $a_{i-1}=b_{i-1}=q_{i-1}=1$, то $\Pr ob_{Q_i^*}=\Pr ob_{Q_{i-1}}$, $\Pr ob_{Q_i^0}=0$,

иначе $\Pr ob_{Q_i}=\frac{1}{2}\Pr ob_{Q_{i-1}}$, где $Q_i^0=(0,q_{i-1},q_{n-2},...,q_0)$, $Q_i^1=(1,q_{i-1},q_{n-2},...,q_0)$,

$Q_i=(q_i,q_{i-1},q_{n-2},...,q_0)$, $q_i\in\{0,1\}$.

Доказательство. Пусть заданы входные числа X и Y для операции сложения по модулю 2^n, $X=(x_{n-1},x_{n-2},....,x_0)$, $Y=(y_{n-1},y_{n-2},....,y_0)$. Для заданных входных разностей A и B, $A=(a_{n-1},a_{n-2},...,a_0)$, $B_{i-1}=(b_{i-1},b_{n-2},...,b_0)$, рассмотрим значение выходной разности Q, $Q=(q_{n-1},q_{n-2},...,q_0):(X\boxplus Y)\oplus((X\oplus A)\boxplus(Y\oplus B))=Q$.

Обозначим через Z, $Z = (z_{n-1}, z_{n-2}, ..., z_0)$ значение выхода операции сложения по модулю 2^n для чисел X и Y: $Z = X \boxplus Y$. Тогда i-бит этого выражения может быть выражен следующим образом: $z_i = x_i \oplus y_i \oplus P_{i-1}$, где P_{i-1} - перенос из i-1 разряда. P_0=0.

Через $Z`$, $Z' = (z'_{n-1}, z'_{n-2}, ...., z'_0)$ обозначим значение выхода операции сложения по модулю $2^n$ для чисел $(X \oplus A)$ и $(Y \oplus B)$: $Z` = (X \oplus A) \boxplus (Y \oplus B)$. В этом случае i-бит выхода равен: $z`_i = x_i \oplus a \oplus y_i \oplus b \oplus P`_{i-1}$, где $P`_{i-1}$ перенос из $i$-1 разряда. $P`_0$ =0.

Значения переносов P_{i-1} и $P`_{i-1}$ могут быть выражены следующим образом: $P_{i-1} = x_{i-1}y_{i-1} \oplus x_{i-1}P_{i-2} \oplus y_{i-1}P_{i-2}$, $P`_{i-1} = (x_{i-1} \oplus a_{i-1})(y_{i-1} \oplus b_{i-1}) \oplus (x_{i-1} \oplus a_{i-1})P`_{i-2} \oplus (y_{i-1} \oplus b_{i-1})P`_{i-2}$.

Тогда i-бит выходной разности для заданных входных разностей A и B (1) будет равен:

$q_i = z_i \oplus z`_i = a_i \oplus b_i \oplus P_{i-1} \oplus P`_{i-1}$. Раскроем скобки в значении переноса $P`_{i-1}$:

$P`_{i-1} = x_{i-1}y_{i-1} \oplus x_{i-1}b_{i-1} \oplus y_{i-1}a_{i-1} \oplus a_{i-1}b_{i-1} \oplus x_{i-1}P`_{i-2} \oplus a_{i-1}P`_{i-2} \oplus y_{i-1}P`_{i-2} \oplus b_{i-1}P`_{i-2}$.

Значения $q_i \oplus a_i \oplus b_i$, полученные используя приведенные выше выражения для $P`_{i-1}$ и приведены в таблице 1.

Таблица 1

Значение $q_i \oplus a_i \oplus b_i$ в зависимости от x_{i-1} и y_{i-1}

x_{i-1}	y_{i-1}	$q_i \oplus a_i \oplus b_i$
0	0	$a_{i-1}b_{i-1} \oplus P`_{i-2}(a_{i-1} \oplus b_{i-1})$
0	1	$a_{i-1}b_{i-1} \oplus P`_{i-2}(a_{i-1} \oplus b_{i-1} \oplus 1) \oplus a_{i-1} \oplus P_{i-2}$
1	0	$a_{i-1}b_{i-1} \oplus P`_{i-2}(a_{i-1} \oplus b_{i-1} \oplus 1) \oplus b_{i-1} \oplus P_{i-2}$
1	1	$a_{i-1}b_{i-1} \oplus P`_{i-2}(a_{i-1} \oplus b_{i-1}) \oplus a_{i-1} \oplus b_{i-1}$

Далее рассмотрим значение $q_i \oplus a_i \oplus b_i$ уже в зависимости от того, чему равны a_{i-1} и b_{i-1}. Значение $q_i \oplus a_i \oplus b_i$, если $a_{i-1} = b_{i-1}$ приведено в таблице 2.

Таблица 2

Значение $q_i \oplus a_i \oplus b_i$ в зависимости от x_{i-1} и y_{i-1}, $a_{i-1} = b_{i-1}$

x_{i-1}	y_{i-1}	$q_i \oplus a_i \oplus b_i$
0	0	$a_{i-1}b_{i-1}$
0	1	$P_{i-2} \oplus P`_{i-2} = q_{i-1}$
1	0	$P_{i-2} \oplus P`_{i-2} = q_{i-1}$
1	1	$a_{i-1}b_{i-1}$

Значение $q_i \oplus a_i \oplus b_i$, если $a_{i-1} \neq b_{i-1}$ приведено в таблице 3.

Таблица 3

Значение $q_i \oplus a_i \oplus b_i$ в зависимости от x_{i-1} и y_{i-1}, $a_{i-1} \neq b_{i-1}$

y_{i-1}	y_{i-1}	$q_i \oplus a_i \oplus b_i$
0	0	$P`_{i-2} = q_{i-1} \oplus P_{i-2} \oplus 1$
0	1	$P_{i-2} \oplus a_{i-1}$
1	0	$P_{i-2} \oplus b_{i-1}$
1	1	$P`_{i-2} \oplus 1 = q_{i-1} \oplus P_{i-2}$

Сводные значения для $q_i \oplus a_i \oplus b_i$, при $\Pr ob_{Q_{i-1}} = C$, приведены в таблице 4.

Таблица 4

Значение $q_i \oplus a_i \oplus b_i$

a_{i-1}	b_{i-1}	q_{i-1}	$q_i \oplus a_i \oplus b_i$	$\Pr ob_{Q_i}$
0	0	0	0	C
			1	0
0	0	1	0	$\frac{C}{2}$
			1	$\frac{C}{2}$
0	1	0	0	$\frac{C}{2}$
			1	$\frac{C}{2}$
0	1	1	0	$\frac{C}{2}$
			1	$\frac{C}{2}$
1	0	0	0	$\frac{C}{2}$
			1	$\frac{C}{2}$
1	0	1	0	$\frac{C}{2}$
			1	$\frac{C}{2}$
1	1	0	0	$\frac{C}{2}$
			1	$\frac{C}{2}$
1	1	1	0	0
			1	C

Далее утверждение теоремы следует из таблицы 4.

Замечание.

Для полученной таблицы 4 вычисления вероятности $\Pr ob_{Q_i}$ требуется задать начальные значения вероятностей $\Pr ob_1$ и $\Pr ob_0$. Начальные значения для вычисления вероятности $\Pr ob_{Q_i}$ представлены в таблице 5.

Таблица 5

Начальные значения для вычисления вероятности $\Pr ob_{Q_i}$

a,b	Q=0	Q=1	Q=2	Q=3
00,00	1	0	0	0
00, 01	0	0.5	0	0.5
00,10	0	0	1	0
00,11	0	0.5	0	0.5
01,00	0	0.5	0	0.5
01,01	0.5	0	0.5	0
01,10	0	0.5	0	0.5
01,11	0.5	0	0.5	0
10,00	0	0	1	0
10,01	0	0.5	0	0.5
10,10	1	0	0	0
10,11	0	0.5	0	0.5
11,00	0	0.5	0	0.5
11,01	0.5	0	0.5	0
11,10	0	0.5	0	0.5
11,11	0.5	0	0.5	0

Исходя из поученных результатов видно, что для того, чтобы рассчитать вероятность распространения разности длины *k* бит, требуется знать вероятность распространения разности длины *k-1* бит. При этом пользуясь теоремой 1 можно не только получить вероятность распространения разностей по модулю 2 через операцию сложения по модулю 2^n, но и получить целые классы невозможных разностей для операции сложения по модулю 2^n.

3. Применение усеченных разностей в криптоанализе *ARX* шифров

Обозначим входные разности для операции сложения по модулю 2^n через A и

B, $A=(a_{n-1},a_{n-2},...,a_0)$, $B=(b_n,b_{n-1},...,b_0)$, а выходную разность через Q, $Q=(q_{n-1},q_{n-2},...,q_0)$. Рассмотрим усеченные разности операции сложения по модулю 2^n. Пусть нам заданы входные усеченные разности $\overline{A}$ и $\overline{B}$ $\overline{A}=(a_k,a_{k-1},...,a_l)$, $\overline{B}=(b_k,b_{k-1},...,b_l)$ длины *k-l*. Пусть U – множество всех выходных усеченных разностей по модулю 2 для операции сложения по модулю 2^n. Обозначим через F, функцию отображения входных усеченных разностей в выходную усеченную разность $F:\overline{A}\times\overline{B}->\overline{Q},\ \overline{A},\overline{B},\overline{Q}\in U$. Причем для этой функции известно, что $\forall i,j\in N,\forall A,B,Q\in U,P(F(A\times B)=Q)=c_{ij},\ c_{ij}\geq 0$. Тогда под действием операции сложения по модулю 2^n разности $\overline{A}$ и $\overline{B}$ переходят во множество выходных разностей Δ, $\Delta=\{\overline{Q}\in U\mid F(\overline{A}\times\overline{B})=\overline{Q}\}$. Согласно теореме 1, разность $\overline{Q}$ в которую переходят входные разности $\overline{A}$ и $\overline{B}$ зависит не только от значения $\overline{A}$ и $\overline{B}$, но так же от того, был ли бит q_{l-1} полной выходной разности Q равен 0 или 1.

Очевидно, что $\forall\overline{A},\overline{B}\ \ F(\overline{A}\times\overline{B})=F(\overline{B}\times\overline{A})$, поэтому в дальнейшем, без ограничения общности можно рассматривать пары входных разностей $(\overline{A},\overline{B})$ без повторения.

Для значения *k-l* равного 1 усеченные разности вырождаются в переходы значения одного бита. Для этого случая $\Delta=\{0,1\}$, причем $P(\overline{Q}=0)=P(\overline{Q}=1),\ \ \overline{Q}\in\Delta$.

Используя усеченные разности, можно строить пути их распространения для конкретных *ARX* схем. При этом сложность перебора всех возможных путей распространения усеченной разности значительно ниже, чем для полного перебора всех путей распространения полной разности. Для *ARX* схемы шифрования, использующей n-битные операции сложения по модулю 2^n вместо построения таблицы перехода для 2^n разностей, требуется построить таблицу для *(k-l-1)/2*, где *(k-l)* – число битов в усеченной разности.

Можно выделить класс *ARX* алгоритмов шифрования, для которого, любой *ARX* шифр, входящий в него может быть атакован с помощью метода усеченных разностей. Для этого сначала докажем 2 утверждения.

Утверждение 1. $\Pr ob(F(2^{k-l}\times 0)=2^{k-l}\mid q_{l-1}=a_{l-1}=b_{l-1}=0)=1,\ \forall k,l\in N.$

Доказательство. Рассмотрим усеченные входные разности по модулю 2 операции сложения по модулю 2^n $\overline{A}$ и $\overline{B}$ $,\overline{A}=(a_k,a_{k-1},...,a_l),\overline{B}=(b_k,b_{k-1},...,b_l)$ усеченную

выходную разность $\overline{Q} = (q_k, q_{k-1}, ..., q_l)$ и полную выходную разность $Q = (q_n, q_{n-1}, ..., q_0)$. Согласно замечанию к теореме 1 для $P((q_0, q_1) = (0,0) \mid (a_0, a_1), (b_0, b_1) = (0,0), (0,0)) = 1$. Тогда, для $i \in \overline{2..k-1}$, если $a_i = a_{i-1} = b_i = b_{i-1} = q_{i-1} = 0$, то согласно теореме 3 $q_i = 0$. Старший бит выходной разности $\overline{Q}$ в этом случае может быть вычислен следующим образом: $q_k = a_k \oplus b_k = 0 \oplus 1 = 1$.

Утверждение 2. $\Pr ob(F(2^{k-l} \times 2^{k-l}) = 0 \mid q_{l-1} = a_{l-1} = b_{l-1} = 0) = 1, \ \forall k, l \in N.$

Доказательство. Аналогично доказательству утверждения 1 рассмотрим усеченные входные разности по модулю 2 операции сложения по модулю 2^n $\overline{A}$ и $\overline{B}$, $\overline{A} = (a_k, a_{k-1}, ..., a_l)$, $\overline{B} = (b_k, b_{k-1}, ..., b_l)$ усеченную выходную разность $\overline{Q} = (q_k, q_{k-1}, ..., q_l)$ и полную выходную разность $Q = (q_n, q_{n-1}, ..., q_0)$. Согласно замечанию к теореме 1 для $P((q_0, q_1) = (0,0) \mid (a_0, a_1), (b_0, b_1) = (0,0), (0,0)) = 1$. Тогда, для $i \in \overline{2..k-1}$, если $a_i = a_{i-1} = b_i = b_{i-1} = q_{i-1} = 0$, то согласно теореме 3 $q_i = 0$. Старший бит выходной разности $\overline{Q}$ в этом случае может быть вычислен следующим образом: $q_k = a_k \oplus b_k = 1 \oplus 1 = 0$.

Теорема 2. Пусть дана схема некоторого алгоритма *ARX* шифрования $ARX : W \otimes K -> W, |W| = 2^m$. Для этой схемы известно, что в ней на каждом раунде шифрования используется операции циклического сдвига на $rot = \{r_1, r_2, ..., r_t\}, \ \forall i \in \{1..t\}, \ r_i = \overline{1...m}$. Всего число операций сложения по модулю 2^n равно *R*. Тогда такой алгоритм может быть атакован с помощью усеченных разностей, если

$$\begin{cases} R < (\frac{mr}{n-r}), r = \min(i) : (r \mid n) \wedge (r \le \min\{r_k\}, k \in \overline{1..t}), i \in N \\ \forall i, j \in \{1..t\}, i \ne j \ , \text{НОД}(r_i, r_j) \ne 1. \end{cases}$$

Доказательство. Рассмотрим входные разности *A* и *B*, $A = (a_{n-1}, a_{n-2}, ..., a_0)$, $B = (b_n, b_{n-1}, ..., b_0)$, и выходную разность *Q*, $Q = (q_{n-1}, q_{n-2}, ..., q_0)$ для ARX, с операцией сложения по модулю 2 в качестве операции разности. Пусть так же нам дано $r = \min(i) : (r \mid n) \wedge (r \le \min\{r_k\}, k \in \overline{1..m}), i \in N$. Тогда представим входную разность *A* и *B*

как конкатенацию усеченных разностей следующим образом: $A=(a_{n-1},a_{n-2},...,a_{n-r+1})\|(a_{n-r},a_{n-2},...,a_{n-2r+1})\|...\|(a_{n-kr},a_{n-2},...,a_0)=\overline{A_1}\|\overline{A_2}\|...\|\overline{A_k}$, $B=$ $=(b_{n-1},b_{n-2},...,b_{n-r+1})\|(b_{n-r},b_{n-2},...,b_{n-2r+1})\|...\|(b_{n-kr},b_{n-2},...,b_0)=\overline{B_1}\|\overline{B_2}\|...\|\overline{B_k}$. При этом начальным значением для каждой из усеченных разностей входа $\overline{A_1},\overline{A_2},...,\overline{A_k},\overline{B_1},\overline{B_2},...,\overline{B_k}\in\{0,2^r\}$. Тогда, согласно утверждению 1 и утверждению 2, каждая входная усеченная разность может под действием функции F отображения входных усеченных разностей по модулю 2 операции сложения по модулю 2^n в некоторую выходную усеченную разность может принять значение либо 0, либо 2^r. Заметим, что операция сложения по модулю 2 для таких усеченных разностей, так же переводит их либо в 0, либо в 2^r. Если $(r\mid n)\wedge(r\le\min\{r_k\},k\in\overline{1..t},i\in N$, то такое распространение разности справедливо вне зависимости от числа операций циклического сдвига в схеме *ARX*. Тогда единственной операцией, которая влияет на выходную разность, является операция сложения по модулю 2^n, причем $P(F(2^{k-l}\times 0)=2^{k-l})=P(F(2^{k-l}\times 2^{k-l})=0)=P(q_{l-1}=0),\quad\forall k,l\in N$. Тогда, очевидно что:

- $\Pr ob(F(0\times 0)=0\mid\overline{A_{i-1}}=0\wedge\overline{B_{i-1}}=0)=1,$
- $\Pr ob(F(0\times 0)=0\mid\overline{A_{i-1}}\neq 0\vee\overline{B_{i-1}}\neq 0)=\frac{1}{2},$
- $\Pr ob(F(2^r\times 0)=2^r\mid\overline{A_{i-1}}=0\wedge\overline{B_{i-1}}=0)=1,$
- $\Pr ob(F(2^r\times 0)=2^r\mid\overline{A_{i-1}}\neq 0\vee\overline{B_{i-1}}\neq 0)=\frac{1}{2},$
- $\Pr ob(F(2^r\times 2^r)=0\mid\overline{A_{i-1}}=0\wedge\overline{B_{i-1}}=0)=1,$
- $\Pr ob(F(2^r\times 2^r)=0\mid\overline{A_{i-1}}\neq 0\vee\overline{B_{i-1}}\neq 0)=\frac{1}{2}.$

Отсюда следует, что $\prod_{i\in\{1,..,k\}}P(F(\overline{A_i}\times\overline{B_i})=\overline{C_i})\le\frac{1}{2^{(\frac{n}{r}-1)}},\overline{C_i}\in\{0,2^r\}$. Тогда в худшем случае входные разности $\overline{A_1},\overline{A_2},...,\overline{A_k},\overline{B_1},\overline{B_2},...,\overline{B_k}\in\{0,2^r\}$ могут быть распространены через одну операцию сложения по модулю 2^n с вероятностью, равной $\frac{1}{2^{(\frac{n}{r}-1)}}$. Если общее число операций сложения по модулю 2^n в *ARX* схеме равно *R*, то она может быть атакована с помощью такого алгоритма, если $R<(\frac{mr}{n-r})$.

4. Выводы

- На основании разностных свойств операции сложения по модулю 2^n был описан класс криптографически не стойких *ARX* шифров;
- Исследование операции сложения по модулю 2^n позволило представить описание эффективного способа подсчета разностной характеристики рассматриваемой операции;
- Полученные результаты могут в дальнейшем использоваться как для более детального изучения *ARX* конструкций в целом, так и для подтверждения уже существующих атак на такие конструкции.

Список литературы

[1]. H. Lipmaa, Wallen J., Dumas P. On the Additive Differential Probability of Exclusive-Or. LNCS. P. 317-331. Springer Berlin Heidelberg. 2004. DOI: 10.1007/978-3-540-25937-4_20.

[2]. Mouha N., Velichkov V., Canniere C. De, Preneel B. The Differential Analysis of S-functions. In D. Stinson, editor, SAC, LNCS, Springer, 2010. P. 36-56.

[3]. Mouha N., Velichkov V., Canniere C. De, Preneel B. The Additive differential probability of ARX. SAC, LNCS. Springer, 2011. P. 342-358.

[4]. Biryukov A., Roy A., Velichkov V. Differential Analysis of Block Ciphers SIMON and SPECK. FSE 2014, LNCS. Springer, 2014.

[5]. Lipmaa H., Wallen J., Dumas P. On the Additive Differential Probability of Exclusive-Or, FSE 2004. V. 3017 of LNCS. Springer, 2004. P. 317–331.