Национальный исследовательский ядерный университет

МИФИ

Кафедра 42 «Криптология и кибербезопасность»

О почти совершенных нелинейных преобразованиях и разделяющем свойстве мультимножеств.

Исполнитель: Сорокин Михаил

студент гр. С14-502

Научный руководитель: Пудовкина М.А.

д.ф.-м.н., профессор

План

- Что такое APN-преобразование;
- Разделяющее свойство и интегральный метод;
- Разделяющее свойство и APN-функции;
- Результаты моих экспериментов.

APN-преобразование

Определение. *Преобразование* $F: GF(2^n) \to GF(2^n)$ *называется APN-преобразованием, если для любых* $a \neq 0$ *из* $GF(2^n)$ *и любых* $b \epsilon GF(2^n)$ *уравнение* $F(x+a) - F(x) = b$ *имеет два или ноль решений*.

Разделяющее свойство

Пусть V_n – множество всех n-мерных битовых векторов, $x[i]$ – i-я координата вектора $x \in V_n$, $i \in \{1, \dots, n\}$. Для каждого элемента $x \in GF(2)$ положим $x^1 = x$, $x^0 = 1$. Тогда корректно определено отображение $\pi: V_n \times V_n \to V_n$, заданное правилом $\pi: (x, u) \mapsto \prod_{i=1}^{n} x[i]^{u[i]}$.

Определение.[Тодо15] Пусть $n \in \mathbb{N}$, $i \in \{1, \dots, n\}$. Говорят, что мультимножество X с носителем V_n имеет разделяющее свойство $D_k^{(n)}$, если $\bigoplus_{x \in X} \pi(x, u) = 0$ для любого фиксированного $u \in (V_n \backslash S_k^{(n)})$, где $S_k^{(n)} = \{a \in V_n : \|a\| \geq k\}$, $\|a\|$ - вес Хэмминга.

Теорема об разделяющем свойстве и S-боксе

Теорема 1.[Тодо15] Пусть $s: GF(2^n) \to GF(2^n)$ – векторная булева функция алгебраической степени *d,* а мультимножество *X* с носителем V_n имеет разделяющее свойство $D_k^{(n)}, n \neq k$. Тогда мультимножество, полученное «применением» *s* к *X,* имеет разделяющее свойство $D_{\lceil k/d \rceil}^{(n)}$.

Интегральный метод

Интегральный различитель — совокупность информации об интегральных свойствах мультимножества на протяжении нескольких раундов зашифрования.

Вектор интегральных свойств — вектор интегральных свойств координатных мультимножеств мультимножества с элементами из векторного пространства.

В случае использования разделяющего свойства при построении интегрального различителя анализируется изменение разделяющего свойства мультимножества (координатных мультимножеств) от раунда к раунду начиная с $D_k^{(n)}$ и оканчивая $D_2^{(n)}$.

Разделяющее свойство и APN

В частности, из теоремы 1 следует, что чем меньше будет отношение $\lceil n/d \rceil$ для n-битного S-бокса с алгебраической степенью d, тем короче будет построенные интегральный различитель по методу Тодо.

Были рассмотрены систематизированные в работе [Тужилин09] APN-преобразования. Вычислялось значение $\lceil n/d \rceil$ и определялось, для каких параметров функций он наименьший. (экспериментальный минимум - 2)

Результаты вычислений

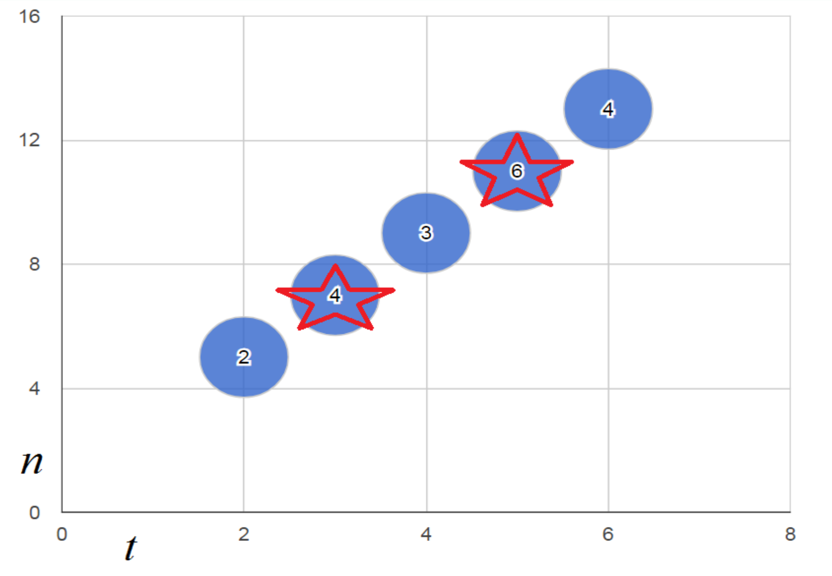

Диаграмма алгебраических степеней APN-функций Нихо
$F(x) = x^j, j = 2^t + 2^{t/2} - 1$, при $2|t$
$j = 2^t + 2^{(3t+1)/2} - 1$ при $t = 2k + 1$
$n = 2t + 1$, $t \in \mathbb{N}$

$\boldsymbol{[n/d] = 2}$ **при** $\boldsymbol{n = 7, t = 3}$ **и** $\boldsymbol{n = 11, t = 5}$.

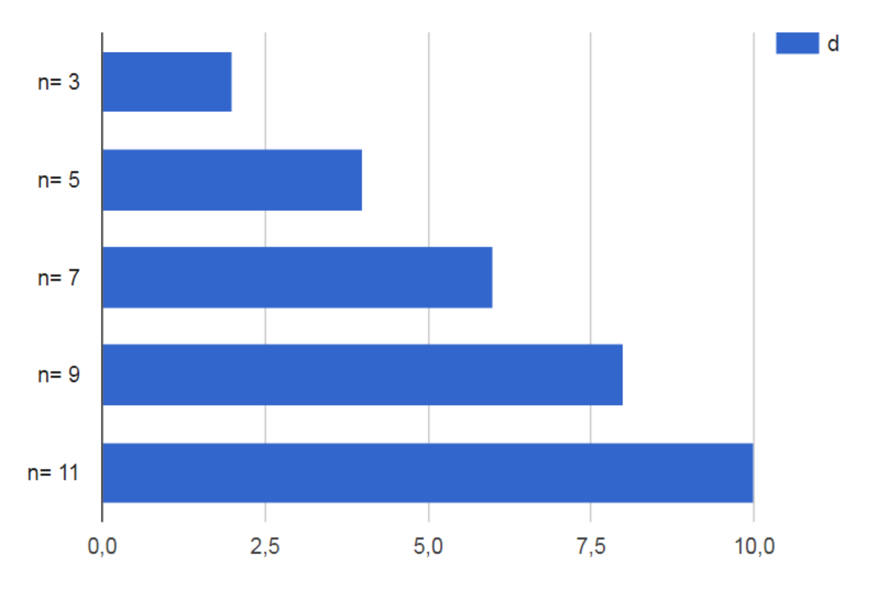

Диаграмма алгебраических степеней APN-функций Клустермана
$F(x) = x^j, j = 2^n - 2$, $n = 2k + 1$, $k \in \mathbb{N}$

Для $\boldsymbol{n \in \{3, \dots, 5\}\ [n/d] = 2}$

Результаты вычислений(1)

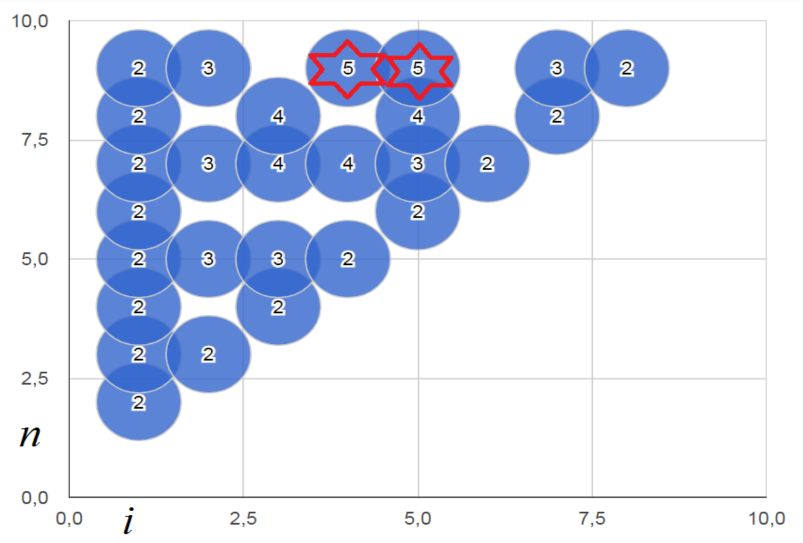

Диаграмма алгебраических степеней APN-функций Касами
$F(x) = x^j, j = 2^{2i} - 2^i + 1$, $\text{НОД}(n, i) = 1$, $\mathrm{i} \in \mathbb{N}$

$\lceil \boldsymbol{n/d} \rceil = \mathbf{2}$ **при** $(\boldsymbol{n}, \boldsymbol{i}) \in \{(\mathbf{9}; \mathbf{4}), (\mathbf{9}; \mathbf{5})\}$

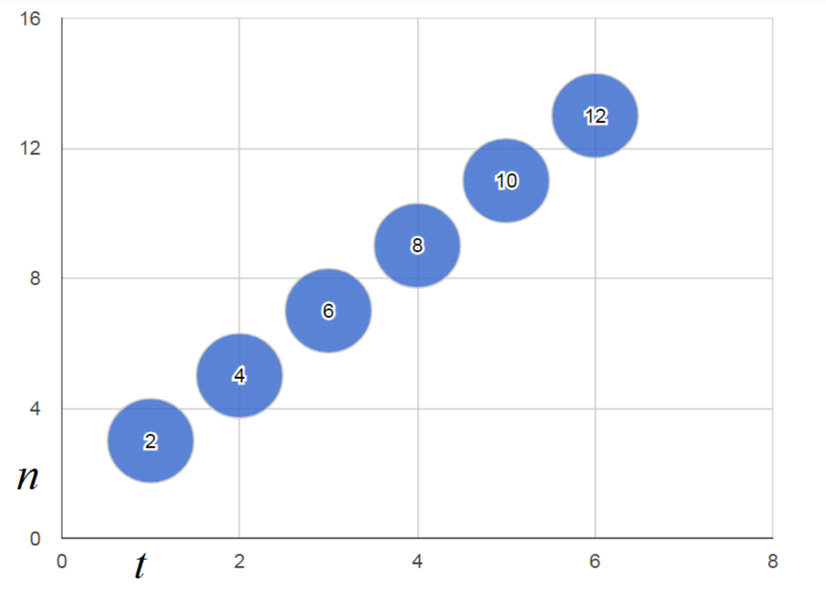

Диаграмма алгебраических степеней APN-функций инверсии
$F(x) = x^j, j = 2^{2t} - 1$, $n = 2t + 1$, $\mathrm{t} \in \mathbb{N}$

$\frac{\boldsymbol{n}}{\boldsymbol{d}} = \mathbf{2}$ **при** $\boldsymbol{t} \in \{\mathbf{1}, \dots, \mathbf{6}\}$

Результаты вычислений(2)

Формула и условия	Параметры	Свойства
$F(x) = x^j, j = 2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1, n = 5i,$ $i \in \mathbb{N}$	$i \in \{1,2\}$	$\lceil n/d \rceil = 2$
$F(x) = \Big(x + tr_{n/3}\left(x^{2(2^i+1)} + x^{4(2^i+1)}\right) + tr(x)$	$n = 6$	$\lceil n/d \rceil = 2$
$F(x) = x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$ $n = 3k, k \in \mathbb{N}$, НОД$(k,3) =$ НОД$(s,3k) = 1, k \geq 4$, $i = sk (mod\ 3)$, $m = 3i$, $ord(w) = 2^{2k} + 2^k + 1$	$n = 12$	$\lceil n/d \rceil = 6$
$F(x) = x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$ $n = 4k$, $k \in \mathbb{N}$, НОД$(k,2) =$ НОД$(s,2k) = 1$, $k \geq 3$, $i = sk (mod\ 4)$, $m = 4i$, $ord(w) = 2^{3k} + 2^{2k} + 2^k + 1$	$n = 12$	$\lceil n/d \rceil = 6$

Результаты вычислений(2)

Формула и условия	Параметры	Свойства
$F(x) = x^j, j = 2^i + 1$ НОД(i, n)=1	При $n \in \{2, \ldots, 12\}$ алгебраическая степень равна $d = 2$	$\lceil n/d \rceil$ растет при увеличении *n*
$F(x) = x^{2^i+1} + \left(x^{2^i} + x + 1\right) tr\left(x^{2^i+1}\right)$ $n \geq 4$, $n = 2k + 1$, $k \in \mathbb{N}$, НОД$(i, n) = 1$	Для $n \in \{4, 6, \ldots, 12\}$ $d = 3$	$\lceil n/d \rceil$ растет при увеличении *n*
$F(x) = x^3 + tr(x^9)$ $n \geq 7$, $n > 2p$ для наименьшего *p*, *такого что* $p > 1, p \neq 3$, НОД$(p, n) = 1$	Для $n \in \{7, 9, 11, 12, 13\}$ $d = 2$	$\lceil n/d \rceil$ растет при увеличении *n*

Выводы

- Не все APN-преобразования оптимальны с точки интегрального метода с использованием разделяющего свойства;
- Однако существуют APN-функции, для которых значение $[n/d] = 2$, что сокращает число раундов в интегральным различителе.