

Санкт-Петербургский Государственный
Университет
Математико-механический факультет
Кафедра системного программирования

Меланич Ольга Юрьевна

Построение нелинейных слабо односторонних функций

Дипломная работа

Допущена к защите:
Заведующий кафедрой:
д.ф.-м.н., проф. А.Н. Терехов

Научный руководитель
доцент кафедры информатики, к.ф.-м.н., доцент Э.А. Гирш

Рецензент
с.н.с. НИИ ИТ СПбГУ, к.ф.-м.н. А.Н. Иванов

Санкт-Петербург
2009

Содержание

1	Введение.	3
2	Общие определения.	5
3	Методы доказательства нижних оценок схемной сложности.	8
3.1	Оценки Ламаньи и Севиджа.	8
3.2	Метод исключения гейтов.	9
4	Некоторые конструкции слабо односторонних функций.	10
4.1	Отправная точка для исследований.	10
4.2	Первый результат.	10
4.3	Семейство слабо односторонних функций порядка 2.	11
4.4	Более сильные гарантии надежности.	17
4.5	Семейство слабо односторонних функций со сколь угодно большой степенью обратной функции	19
4.6	Дальнейшие попытки улучшения константы.	22
5	Надежная в слабом смысле функция с секретом.	24
6	Заключение.	26
6.1	Результаты.	26
6.2	Направления дальнейших исследований.	26
	Список литературы.	28

1 Введение.

В 1976 году Уитфилдом Диффи и Мартином Хеллманом были сформулированы основы криптографии с открытым ключом. Основная идея заключается в том, что для шифрования и дешифрования информации могут быть использованы разные ключи, причем ключ для шифрования может быть открытым, или “публичным”. Базовым примитивом в реализации этой идеи послужила *односторонняя функция*. В своей статье “Новые направления в криптографии” Диффи и Хеллман дают математически не строгое, зато интуитивно понятное определение: “Функция f является односторонней, если для любого аргумента x из области определения f легко подсчитать соответствующее значение $f(x)$, но для почти всех y из множества значений f уравнение $y = f(x)$ вычислительно неразрешимо для любого подходящего x ”. Сама по себе односторонняя функция в алгоритмах шифрования с открытым ключом не применима, так как зашифрованную с ее помощью информацию не смогут расшифровать не только взломщики, но те, кому эта информация адресована. Для этих целей используются *функции с секретом*. Неформально: функция с секретом – это такая функция, которую легко вычислять, трудно обращать, не зная некоторой дополнительной информации (“секрета”), и легко обращать, зная “секрет”. (На более формальном языке “легко” обычно означает “за полиномиальное время”, а “трудно” или “вычислительно неразрешимо” – “неразрешимо за полиномиальное время”). В классической криптографии односторонние функции являются базовыми примитивами для протоколов согласования ключа и цифровой подписи, а функции с секретом – базовыми примитивами для криптосистем с открытым ключом.

С тех пор было разработано большое количество различных криптографических протоколов с открытым ключом, однако до сих пор не существует никаких доказательств их надежности. В частности, ни про одну функцию, реально используемую в криптографии, не доказано, что она является односторонней функцией или функцией с секретом. И пока что не видно никаких особых предпосылок к тому, чтобы эти доказательства появились в ближайшее время.

Если мы не умеем доказывать сверхполиномиальную разницу между сложностью честных участников протокола и сложностью взломщика, то почему бы пока не попробовать доказать хоть какую-нибудь разницу? В 1992 году Ален Хильтген [Hil92] сумел построить функцию, обратить которую вдвое сложнее, чем вычислить. Его пример представляет собой линейную функцию над $GF(2)$ с матрицей, у которой мало ненулевых элементов, но зато в обратной к ней ненулевых элементов

много. В качестве модели вычислений у него рассматривается самая общая модель: количество гейтов в булевой схеме с произвольными бинарными гейтами.

В 2008 году Э.А.Гирш и С.И.Николенко [HN08] предложили конструкцию другого криптографического примитива, надежного в слабом смысле: надежную в слабом смысле функцию с секретом. Эта конструкция основывалась на линейной функции Хильтгена. Сложность обращения (декодирования) полученной функции без использования секретной информации по меньшей мере в $\frac{25}{22}$ раза больше, чем сложности честного кодирования, декодирования и генерации ключей. Также для этой конструкции было показано, что более слабый противник (использующий меньшее количество гейтов) не способен обратить эту функцию на хотя бы четверти входов. Полученный результат позволил создать схему с суперполиномиальными гарантиями надежности против более слабых соперников.

Данная работа является продолжением исследований Хильтгена, Гирша и Николенко. Стоит заметить, что линейные функции обратимы с помощью методов линейной алгебры и поэтому в принципе не могут быть односторонними и использоваться в криптографических протоколах. Поэтому основной целью моей работы является построение и исследование именно нелинейных функций, односторонних в слабом смысле.

В разделе 2 даются базовые определения. В разделе 3 производится обзор известных методов доказательства нижних оценок схемной сложности, которые использовались у Хильтгена, Гирша и Николенко. Эти же методы будут использоваться для доказательства нижних оценок в настоящей работе. В разделе 4 приводятся некоторые конструкции нелинейных слабо односторонних функций и доказываются соответствующие порядки необратимости. В разделе 5 приводится конструкция надежной в слабом смысле функции с секретом, построенной на основе слабо односторонней функции из предыдущего раздела. В разделе 6 коротко формулируются достигнутые результаты и предлагаются направления дальнейших исследований.

2 Общие определения.

Обозначим через $B_{n,m}$ множество всех 2^{m2^n} функций $f : B^n \rightarrow B^m$, где $B = \{0, 1\}$ – поле из двух элементов. Нашей вычислительной моделью являются булевские схемы с произвольными бинарными гейтами.

Определение 1. *Булевская схема* – это ациклический направленный граф, каждая вершина которого либо не имеет ни одного входящего ребра (такие вершины называются *входами* схемы, или *переменными*), или два входящих ребра (такие вершины называются *гейтами*). Каждый гейт помечен бинарной булевой функцией, то есть любой из шестнадцати функций из $B_{2,1}$. Некоторые гейты помечены как *выходы* (по техническим причинам также допускается, что выходом может быть отрицание вычисляемого в гейте значения; таким образом можно избежать лишних гейтов-отрицаний). Также выходом может быть вход или отрицание входа. Схема с n входами и m выходами естественным образом вычисляет функцию из $B_{n,m}$. Размер схемы мы будем обозначать как $Size$.

Определение 2. *Схемная сложность* (или просто *сложность*) функции f , обозначаемая через $C(f)$, – это наименьшее количество гейтов в схеме, вычисляющей f , то есть

$$C(f) = \min_{c: \forall x c(x) = f(x)} Size(c).$$

Такая схема называется *оптимальной схемой* для функции f . Можно без потери общности предполагать, что каждый гейт схемы нетривиально зависит от обоих входов, то есть что в схеме нет функций-констант и унарных функций Id и NOT , потому что такие гейты легко исключить из схемы, не увеличивая количество гейтов в ней.

Через $C_\delta(f)$ будем обозначать минимальный размер схемы, которая вычисляет f на более чем δ -й доле входов.

А. Хильтген ввел для каждой обратимой (инъективной) функции $f_n \in B_{n,n}$ понятие *меры сложности в слабом смысле (measure of feeble one-wayness)*

$$M_F(f_n) = \frac{C(f_n^{-1})}{C(f_n)}$$

Результаты Хильтгена заключались в том, что он нашел последовательности функций $\{f_n\}_{n=1}^\infty$ с нетривиальными константами

$$\liminf_{n \rightarrow \infty} M_F(f_n),$$

которые Хильтген называет порядком необратимости (*order of one-wayness*).

Определение 3. Семейство функций f_n является *слабо односторонним порядка k* (*feebly-one-way of order k*), если $\liminf_{n \rightarrow \infty} (f_n) = \infty$ и $\liminf_{n \rightarrow \infty} M_F(f_n) = k$ при $k > 1$ и не обязательно конечном.

Далее я практически дословно приведу основные определения (с соответствующими замечаниями и пояснениями), введенные Э. А. Гиршем и С. И. Николенко касательно надежных в слабом смысле функций с секретом.

Определение 4. Семейство кандидатов в функции с секретом – это тройка

$$C = \{Key_n, Eval_n, Inv_n\},$$

где:

- Key_n – это семейство сэмплирующих схем $Key_n : B^n \rightarrow B^{pi(n)} \times B^{ti(n)}$,
- $Eval_n$ – это семейство вычисляющих функцию схем $Eval_n : B^{pi(n)} \times B^{m(n)} \rightarrow B^{c(n)}$, а
- Inv_n – это семейство обращающих функцию схем $Inv_n : B^{ti(n)} \times B^{c(n)} \rightarrow B^{m(n)}$,

причем для каждого n , каждого начального числа генератора $s \in B_n$ и каждого сообщения $m \in B^{m(n)}$

$$Inv_n(Key_{n,2}(s), Eval_n(Key_{n,1}(s), m)) = m,$$

где $Key_{n,1}(s)$ и $Key_{n,2}(s)$ – первые $pi(n)$ битов (“публичная информация”, *public information*) и последние $ti(n)$ битов (“секрет”, *trapdoor information*) выхода схемы $Key_n(s)$, соответственно.

Число n – это параметр надежности, длина начального числа генератора случайных чисел. Длину входа функции обозначается через $m(n)$, через $c(n)$ – длину ее выхода, а через $pi(n)$ и $ti(n)$ – длину публичной информации и секрета соответственно. Такое семейство функций называется “кандидатом”, потому что в определении ничего не говорится о надежности, а только вводятся обозначения для размерностей и устанавливается корректность обращения.

Определение 5. Схема N успешно обращает семейство кандидатов в функции с секретом f на входах длины n , если для равномерного распределения U , взятого по начальным числам генератора $s \in B^n$ и входам $m \in B^{m(n)}$,

$$Pr_{s,m \in U}[N(Key_{n,1}(s), Eval_n(Key_{n,1}(s), m)) = m] > \frac{7}{8}.$$

Замечание 1. У Гирша и Николенко в этом определении вместо $\frac{7}{8}$ используется константа $\frac{3}{4}$. Но это не имеет принципиального значения,

так как далее в настоящей работе будет построено семейство с гораздо более сильными гарантиями надежности.

Определение 6. Семейство кандидатов в функции с секретом f имеет *порядок надежности* k , если для каждой последовательности схем $\{N_n\}_{n=1}^\infty$, которые успешно обращают f на каждой длине входа n ,

$$\liminf_{i \rightarrow \infty} \min \left\{ \frac{Size(N_n)}{C(Key_n)}, \frac{Size(N_n)}{C(Eval_n)}, \frac{Size(N_n)}{C(Inv_n)} \right\} \geq k.$$

Замечание 2. Следует явно отметить, что речь идет исключительно об одновременной надежности. Противник может использовать меньшее количество гейтов, обращая семейство кандидатов в функции с секретом второй раз для той же пары ключей: например, он может вычислить секретную информацию и успешно использовать ее вторично. Таким образом, в предлагаемых конструкциях требуется для каждого нового входа выбирать новую пару ключей (фактически, новое начальное число генератора).

3 Методы доказательства нижних оценок схемной сложности.

3.1 Оценки Ламаньи и Севиджа.

Ален Хильтген доказал все свои оценки при помощи следующих утверждений, впервых сформулированных Ламаньей и Севиджем.

Предложение 1. ([LS73,Sav76]; [Hil92, Теоремы 3 и 4]; [HN08, Предложение 1])

1. Предположим, что функция $f : B^n \rightarrow B$ нетривиально зависит от каждой из n своих переменных, то есть для любого i найдутся такие значения $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n \in B$, что $f(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n)$. Тогда $C(f) \geq n - 1$.
2. Пусть $f = (f^{(1)}, \dots, f^{(m)}) : B^n \rightarrow B^m$, где $f^{(k)}$ – это k -я компонента функции f . Если все m функций-компонент $f^{(i)}$ попарно различны, и для каждой из них $C(f^{(i)}) \geq c > 1$, то $C(f) \geq c + m - 1$.

Доказательство.

1. Рассмотрим минимальную схему размера s , вычисляющую f . Поскольку f нетривиально зависит от всех n своих переменных, у каждого из входов схемы должно быть по крайней мере одно исходящее ребро. Поскольку схема минимальна, у каждого из оставшихся гейтов в ней, кроме, возможно, выхода, тоже должно быть по крайней мере одно исходящее ребро. Поэтому в схеме должно быть по крайней мере $s + n - 1$ ребер. С другой стороны, в схеме из s бинарных гейтов не может быть более чем $2s$ ребер. Поэтому $2s \geq s + n - 1$.
2. Рассмотрим схему, вычисляющую f . Отметим, что в ней есть по меньшей мере $c - 1$ гейтов, не вычисляющих никакую функцию схемной сложности c или более (в качестве таких гейтов можно рассмотреть первые $c - 1$ гейтов в каком-либо топологическом порядке). Но для вычисления любой функции-компоненты $f^{(i)}$ требуется добавить по меньшей мере еще один гейт, причем потребуется добавлять по одному гейту для каждой компоненты, ведь один новый гейт добавляет только одну новую функцию. Так и получается необходимая оценка в $c + m - 1$ гейтов.

□

3.2 Метод исключения гейтов.

Метод *исключения гейтов* (*gate elimination*) применялся в доказательстве основной леммы у Гирша и Николенко, а также практически во всех доказательствах нижних оценок на размеры схем произвольного вида.

Суть метода состоит в том, чтобы последовательно подставлять определенные значения вместо некоторых переменных таким образом, чтобы при этом в итоге из схемы “исключилось” как можно больше гейтов. Когда мы подставляем в f значение $x = a$, в схеме, вычисляющей f , все гейты, в которые входит x , становятся либо константными, либо унарными. Если гейт стал унарным, то его можно исключить из схемы, так как он представляет собой либо Id , либо его отрицание, а отрицание можно перенести на следующие бинарные гейты, немного изменив функции, которые в них вычислялись. Если гейт стал константным, то все его потомки стали константными или унарными, а значит, можно исключить и сам этот гейт, и его потомков. Если гейт нелинеен, то подстановкой вместо любой из переменных подходящей константы можно добиться того, чтобы гейт стал константным. Если гейт линеен, то при подстановке любого значения любой из переменных он станет унарным. Также иногда бывает полезно подставлять вместо x не константу, а какую-нибудь функцию. Например, когда единственный гейт g , в которой входит x , линеен, а хочется исключить одной подстановкой сразу как минимум два гейта, можно подставить вместо x функцию, которая является вторым входом g (этот прием будет использован в настоящей работе). Количество исключенных гейтов дает нижнюю оценку на схемную сложность f . Стоит отметить, что от этого метода трудно ожидать более чем линейных оценок.

4 Некоторые конструкции слабо односторонних функций.

4.1 Отправная точка для исследований.

В 1990 году Хильтген и Ганц методом полного перебора показали, что для всех функций из $B_{1,1}$, $B_{2,2}$ и $B_{3,3}$ сложность обратной функции совпадает со сложностью прямой ([Mas96], слайд 18), и нашли первую функцию, обратить которую сложнее, чем вычислить.

$$\begin{array}{ll} y_1 = x_1 \oplus x_3 & x_1 = [(y_1 \oplus y_3) \oplus y_2]y_4 \oplus (y_1 \oplus y_3) \\ y_2 = x_2 \oplus [(x_1 \oplus x_2)x_4] & x_2 = [(y_1 \oplus y_3) \oplus y_2]y_4 \oplus y_2 \\ y_3 = x_3 \oplus [(x_1 \oplus x_2)x_4] & x_3 = [(y_1 \oplus y_3) \oplus y_2]y_4 \oplus y_3 \\ y_4 = x_4 & x_4 = y_4 \\ C(f) = 5 & C(f^{-1}) = 6 \end{array}$$

4.2 Первый результат.

Мои исследования нелинейных функций начались с попыток обобщения этого примера. Первой удачной конструкцией стала последовательность функций от $(3k+1)$ переменной $\{f_{3k+1}\}_{k=1}^{\infty}$, имеющих следующий вид.

$$\begin{aligned} y_i &= \Pi \oplus x_{2i-1} \\ y_{k+j} &= \Pi \oplus x_{2k+j} \\ y_{2k+l} &= x_{2k+l} \oplus x_{2l} \\ y_{3k+1} &= x_{3k+1}, \end{aligned}$$

где $i, j, l \in [1..k]$, а $\Pi = (x_1 \oplus x_2) \cdot \dots \cdot (x_{2k-1} \oplus x_{2k})x_{3k+1}$.

Для того, чтобы получить f_{3k+1}^{-1} , для каждого $i \in [1..k]$ сложим строки, соответствующие y_i, y_{k+i}, y_{2k+i} .

$$y_i \oplus y_{k+i} \oplus y_{2k+i} = \Pi \oplus x_{2i-1} \oplus \Pi \oplus x_{2k+i} \oplus x_{2k+i} \oplus x_{2i} = x_{2i-1} \oplus x_{2i}$$

Тогда $\Pi = (\prod_{i=1}^k (y_i \oplus y_{k+i} \oplus y_{2k+i}))y_{3k+1}$ и обратная функция имеет вид:

$$\begin{aligned} x_{2i-1} &= \Pi \oplus y_i \\ x_{2k+j} &= \Pi \oplus y_{k+j} \\ x_{2l} &= x_{2k+l} \oplus y_{2k+l} = \Pi \oplus y_{k+l} \oplus y_{2k+l} \\ x_{3k+1} &= y_{3k+1}, \end{aligned}$$

где $i, j, l \in [1..k]$.

Утверждение 1. $4k - 1 \leq C(f_{3k+1}) \leq 5k$.

Доказательство. Выражение Π нетривиально зависит от $2k + 1$ переменной и поэтому вычисляется минимум $2k$ гейтами (при этом ровно за $2k$ можно). Значит, $\forall i \in [1..2k] C(y_i) \geq 2k$. Поскольку первые $2k$ компонентных функций различны, $C(f_{3k+1}) \geq 2k + (2k - 1)$. Если Π подсчитано, то для вычисления каждой компонентной функции, кроме последней, достаточно одного гейта, поэтому за $2k + 3k = 5k$ вычислить можно.

□

Утверждение 2. $6k - 1 \leq C(f_{3k+1}^{-1}) \leq 6k$.

Доказательство. Аналогично заметим, что $\forall i \in [1..3k] x_i$ нетривиально зависит от всех $(3k + 1)$ переменных. Поэтому $C(x_i) \geq 3k$. Поскольку первые $3k$ компонентных функций различны, $C(f_{3k+1}^{-1}) \geq 3k + (3k - 1)$. При этом за $6k$ обратная функция считается ($3k$ операций на Π и $3k$ на все остальное).

□

Теорема 1. *Последовательность функций $\{f_{3k+1}\}_{k=1}^{\infty}$ имеет порядок необратимости не менее 1.2 и не более 1.5.*

Доказательство. Непосредственно следует из предыдущих утверждений.

$$\liminf_{k \rightarrow \infty} \frac{6k - 1}{5k} = 1.2.$$

$$\liminf_{k \rightarrow \infty} \frac{6k}{4k - 1} = 1.5.$$

□

4.3 Семейство слабо односторонних функций порядка 2.

Этот пример был получен путем объединения линейной функции Хильтгена [Hil92] с порядком необратимости $\frac{3}{2}$ (были идеи улучшить это семейство, используя функцию Хильтгена с порядком необратимости 2, но они не увенчались успехом, так как построенное мной семейство использует тот кусок функции Хильтгена, на который улучшение им константы до 2 принципиально не повлияло) с квадратичной функцией от четырех переменных, придуманный Хильтгеном и Ганцом.

Рассмотрим последовательность функций $\{f_n\}_{n=1}^{\infty}$, имеющих следующий вид:

$$\begin{aligned} y_1 &= (x_1 \oplus x_2)x_n \oplus x_{n-1} \\ y_2 &= (x_1 \oplus x_2)x_n \oplus x_2 \\ y_3 &= x_1 \oplus x_3 \\ y_4 &= x_3 \oplus x_4 \\ &\dots \\ y_{n-1} &= x_{n-2} \oplus x_{n-1} \\ y_n &= x_n \end{aligned}$$

Для того, чтобы получить f_n^{-1} , сложим все строки, кроме последней.

$$y_1 \oplus \dots \oplus y_{n-1} = x_1 \oplus x_2$$

Далее, подставляя y_n вместо x_n , находим x_2 и x_{n-1} . Остальные x_k -е выражаются через x_{n-1} по цепочке и обратная функция имеет вид:

$$\begin{aligned} x_n &= y_n \\ x_2 &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_2 \\ x_{n-1} &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_1 \\ x_{n-2} &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_1 \oplus y_{n-1} \\ x_{n-3} &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_1 \oplus y_{n-1} \oplus y_{n-2} \\ &\dots \\ x_3 &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_1 \oplus y_{n-1} \oplus \dots \oplus y_4 \\ x_1 &= (y_1 \oplus \dots \oplus y_{n-1})y_n \oplus y_1 \oplus y_{n-1} \oplus \dots \oplus y_3 \end{aligned}$$

Теорема 2. Последовательность функций $\{f_n\}_{n=1}^{\infty}$ имеет порядок необратимости 2.

Доказательство. Нетрудно видеть, что f_n считается за $n+1$ гейт. У f_n^{-1} каждая компонентная функция кроме последней нетривиально зависит от всех n переменных и все компонентные функции различны. Поэтому для вычисления f_n^{-1} требуется как минимум $(n-1) + (n-2) = 2n-3$ гейта. Значит,

$$M_F(f_n) \geq \frac{2n-3}{n+1}.$$

С другой стороны, f_n нельзя вычислить быстрее, чем за $n-1$ гейт, так как все компонентные функции f_n различны и только одна из них тривиальна (зависит только от одной переменной). В то же время f_n^{-1} можно вычислить за $2n-2$ гейта: за $n-1$ вычисляется $(y_1 \oplus \dots \oplus y_{n-1})y_n$

и по одному гейту тратится на довычисление каждой компонентной функции, кроме последней. Отсюда получаем

$$\frac{2n-3}{n+1} \leq M_F(f_n) \leq \frac{2n-2}{n-1}.$$

Устремляя n к бесконечности, получаем требуемое.

□

В криптографии обычно желательно доказать не только оценки в худшем случае, но также тот факт, что противник неспособен обратить функцию на значительной доле ее входов. Во-первых, стоит признать, что существует схема, вычисляющая f_n^{-1} на хотя бы примерно $\frac{3}{4}$ входов всего за $n-3$ гейта. На самом деле эта схема вычисляет линейную часть f_n^{-1} :

$$\begin{aligned} x_1 &= y_1 \oplus y_{n-1} \oplus \dots \oplus y_3 \\ x_2 &= y_2 \\ x_3 &= y_1 \oplus y_{n-1} \oplus \dots \oplus y_4 \\ x_4 &= y_1 \oplus y_{n-1} \oplus \dots \oplus y_5 \\ &\dots \\ x_{n-3} &= y_1 \oplus y_{n-1} \oplus y_{n-2} \\ x_{n-2} &= y_1 \oplus y_{n-1} \\ x_{n-1} &= y_1 \\ x_n &= y_n \end{aligned}$$

“Примерно $\frac{3}{4}$ ” получаются, когда $(y_1 \oplus \dots \oplus y_{n-1})y_n = 0$. А это бывает, когда либо $y_n = 0$ (половина входов), либо среди $y_1, \dots, y_{n-1}$ четное число единиц (при четном n это ровно четверть всех входов, при нечетном почти четверть). Во-вторых, можно доказать, что схема, обращающая f_n на более чем $\frac{7}{8}$ ее входов, содержит хотя бы $2n-4$ гейта. Прежде чем доказывать этот факт, докажем два вспомогательных утверждения.

Утверждение 3. ([HN08], Лемма 3) *Рассмотрим функцию $f = \bigoplus_{i=1}^n x_i$. Для каждой функции g , которая нетривиально зависит только от m из этих переменных при $m < n$,*

$$Pr_{x_1, \dots, x_n}[f(x_1, \dots, x_n) = g(x_{i_1}, \dots, x_{i_m})] = \frac{1}{2}.$$

Доказательство. Поскольку $m < n$, существует такой номер $j \in 1..n$, что g не зависит от x_j . Это значит, что для каждого набора значений всех остальных переменных для одного из значений x_j результат вычисления g совпадает с результатом f , а для другого значения не совпадает. Это значит, что f отличается от g в точности на $\frac{1}{2}$ своих входов.

□

Утверждение 4. В схеме, вычисляющей $f_n^{-1}|_{y_{i_1}=a_1, \dots, y_{i_l}=a_l}$ при $l \leq n-3$, $n \notin \{i_1, \dots, i_l\}$ и $a_i \in \{0, 1, y_n, y_n \oplus 1\}$ на более чем $\frac{3}{4}$ входов, ни одна из переменных, кроме, возможно, y_n , не является выходом схемы и входит хотя бы в один гейт.

Доказательство. В начале заметим, что для $i \neq n$

$$x_i|_{y_k=y_n} = (y_1 \oplus \dots \oplus y_{k-1} \oplus y_n \oplus y_{k+1} \oplus \dots \oplus y_{n-1})y_n \oplus \dots = \\ (y_1 \oplus \dots \oplus y_{k-1} \oplus 1 \oplus y_{k+1} \oplus \dots \oplus y_{n-1})y_n \oplus \dots = x_i|_{y_k=1},$$

если y_k изначально не входил в x_i . Аналогично при подстановках $y_k = y_n$ при линейной части x_i , зависящей от y_k , и $y_k = y_n \oplus 1$ x_i будет в итоге выглядеть так, как будто было подставлено значение из $\{0, 1\}$.

Будем доказывать от противного. Обозначим функцию, которую схема вычисляет на самом деле, за h . Пусть $h_k = y_j$ – выход схемы. Так как $l \leq n-3$, этот выход не зависит как минимум от одной переменной, отличной от y_n . Обозначим ее за y_i . Возможны три случая.

1. $k = n \Rightarrow x_k = y_n$.

Рассмотрим два различных значения переменной y_n (0 и 1) и зафиксируем значения всех остальных переменных. Для одного из значений y_n функция h будет непременно давать неверный ответ, потому что

$$h_n|_{y_n=0} = h_n|_{y_n=1}$$

(h_n не зависит от y_n), а

$$x_n|_{y_n=0} \neq x_n|_{y_n=1},$$

Таким образом, мы получили, что h отличается от f_n^{-1} хотя бы на $\frac{1}{2}$ входов.

2. $x_k = (y_i \oplus \dots)y_n \oplus \bigoplus_{z \in Z} z$, где $y_i \notin Z$.

Рассмотрим два различных значения переменной y_i (0 и 1). Для каждого фиксированного набора значений остальных переменных, в котором $y_n = 1$, для одного из значений y_i функция h будет непременно давать неверный ответ, так как

$$h_k(y_n = 1, y_i = 0, \dots) = h_k(y_n = 1, y_i = 1, \dots),$$

а

$$x_k(y_n = 1, y_i = 0, \dots) \neq x_k(y_n = 1, y_i = 1, \dots),$$

потому что $x_k|_{y_n=1} = y_i \oplus \dots$

Таким образом, мы получили, что h отличается от f_n^{-1} хотя бы на $\frac{1}{4}$ входов. Противоречие.

3. $x_k = (y_i \oplus \dots)y_n \oplus y_i \oplus \dots$

Аналогично предыдущему случаю имеем

$$h_k(y_n = 0, y_i = 0, \dots) = h_k(y_n = 0, y_i = 1, \dots),$$

а

$$x_k(y_n = 0, y_i = 0, \dots) \neq x_k(y_n = 0, y_i = 1, \dots),$$

потому что $x_k|_{y_n=1} = y_i \oplus \dots$, и тем же образом приходим к противоречию.

Теперь докажем вторую часть утверждения. Пусть y_j не входит ни в один гейт и не является выходом, то есть h вообще не зависит от y_j . По построению f_n^{-1} существует $x_k = (y_j \oplus \dots)y_n \oplus y_j \oplus \dots$. Тогда

$$h_k(y_n = 0, y_j = 0, \dots) = h_k(y_n = 0, y_j = 1, \dots),$$

а

$$x_k(y_n = 0, y_j = 0, \dots) \neq x_k(y_n = 0, y_j = 1, \dots),$$

что дает отличие между h и f_n^{-1} на как минимум $\frac{1}{4}$ входов и приводит к противоречию.

□

Теорема 3. $C_{7/8}(f_n^{-1}) \geq 2n - 4$.

Доказательство.¹ Рассмотрим оптимальную схему, вычисляющую f_n^{-1} на более чем $\frac{7}{8}$ входов. Обозначим функцию, которую схема вычисляет на самом деле, через h .

Пусть g – гейт, входы в который ведут из вершин схемы y_i и y_j . Возможны следующие случаи.

1. Одна из переменных, входящих в g , отличная от y_n (например, y_i), входит также в какой-нибудь другой гейт. В этом случае, подставив любое значение вместо y_i , мы сможем исключить два гейта. Заметим, что если h совпадала с f_n^{-1} на более чем $\frac{7}{8}$ всех входов, то либо $h|_{y_i=0}$, либо $h|_{y_i=1}$ будет совпадать с соответствующим сужением f_n^{-1} на более чем $\frac{7}{8}$ оставшихся входов.

¹Это доказательство идеологически повторяет доказательство леммы 5 из [HN08] с некоторыми поправками на нелинейность f_n^{-1}

2. y_i и y_j отличны от y_n и ни y_i , ни y_j не подаются на вход другим гейтам. В этом случае h не зависит от y_i или y_j по отдельности, а зависит только от $g(y_i, y_j)$ (так как ни y_i , ни y_j не являются выходами по утверждению 4). Покажем, что такое невозможно. По построению f_n^{-1} существует выход $x_k = (y_i \oplus y_j \oplus \dots) y_n \oplus y_i \oplus \bigoplus_{z \in Z} z$, где $y_j \notin Z$ (заметим, что это верно и после подстановки значений нескольких переменных). Так как в оптимальной схеме каждый гейт нетривиально зависит от обоих своих входов, существуют значения a и b , такие что $g(0, a) = g(1, b)$. Возможны два случая.

(а) h_k зависит от $g(y_i, y_j)$. Тогда

$$h_k(y_i = 0, y_j = a, y_n = 0, \dots) = h_k(y_i = 1, y_j = b, y_n = 0, \dots),$$

а

$$x_k(y_i = 0, y_j = a, y_n = 0, \dots) \neq x_k(y_i = 1, y_j = b, y_n = 0, \dots),$$

поэтому h отличается от f_n^{-1} хотя бы на $\frac{1}{8}$ входов. Противоречие.

(б) h_k не зависит ни от y_i , ни от y_j . Тогда

$$h_k(y_i = 0, y_n = 0, \dots) = h_k(y_i = 1, y_n = 0, \dots),$$

а

$$x_k(y_i = 0, y_n = 0, \dots) \neq x_k(y_i = 1, y_n = 0, \dots),$$

поэтому h отличается от f_n^{-1} хотя бы на $\frac{1}{4}$ входов. Противоречие.

3. Не умаляя общности, $j = n$ и y_i не подается на вход другим гейтам и g линеен. Покажем, что такое невозможно. Действительно, иначе при подходящем значении y_n ни один из выходов не зависел бы от y_i . По построению f_n^{-1} при любом значении y_n найдется выход $x_k = y_i \oplus \dots$. Тогда

$$h_k(y_i = 0, y_n = a, \dots) = h_k(y_i = 1, y_n = a, \dots),$$

а

$$x_k(y_i = 0, y_n = a, \dots) \neq x_k(y_i = 1, y_n = a, \dots),$$

поэтому h отличается от f_n^{-1} хотя бы на $\frac{1}{4}$ входов. Противоречие.

4. Не умаляя общности, $j = n$ и y_i не подается на вход другим гейтам и g линеен. Если g является выходом схемы h_k , то это означает, что мы уже подставили значения для $n - 2$ переменных, исключили при этом $2n - 4$ гейта и тем самым доказали теорему (в противном случае либо существует y_l такой, что при каком-то значении y_n $x_k = y_l \oplus \dots$, либо $k = n$; и то и другое известным образом ведет к противоречию). Пусть у g есть потомки. Сделаем ту из подстановок $y_i = y_n$ или $y_i = y_n \oplus 1$, при которой h будет по-прежнему совпадать с f_n^{-1} на более чем $\frac{7}{8}$ входов. Этим мы исключаем и сам гейт g и его потомков, то есть как минимум 2 гейта.

Таким образом, пока есть как минимум две переменные, отличные от y_n , и y_n , мы можем исключать по меньшей мере два гейта после подстановки одной переменной так чтобы h совпадала с f_n^{-1} на более чем $\frac{7}{8}$ оставшихся входов; будем называть такие переменные “хорошими”. Подставив все “хорошие” переменные, мы исключим как минимум $2n - 4$ гейта.

□

4.4 Более сильные гарантии надежности.

В предыдущем разделе было показано, что противник, у которого есть меньше, чем $2n - 4$ гейта не способен обратить f_n на более чем $\frac{7}{8}$ всех входов. На основании этого утверждения можно построить функцию с существенно более сильными гарантиями надежности. Сначала докажем некоторое предварительное утверждение.

Утверждение 5. $H : B^{mn} \rightarrow B^{mn}$ определяется так: область определения последовательно бьется на t блоков по n переменных и к каждому такому блоку применяется f_n^{-1} . Тогда $C(H) \geq t(2n - 4)$ и, более того, $C_{7/8}(H) \geq t(2n - 4)$.

Доказательство. Проводим индуктивное рассуждение, аналогичное приведенному в предыдущей теореме. Заметим, что оба случая, все случаи, которые там рассматривались, а также утверждение 4, остаются справедливыми в общем контексте, если рассматриваемые переменные принадлежат одному блоку. Рассмотрим еще четыре важных возможности для верхнего гейта g .

1. Входы g y_i и y_j лежат в разных блоках, y_i входит еще в один гейт и при этом y_i не является “ y_n для своего блока” (иными словами, i не делится на n). Тогда мы можем причислить y_i к “хорошим” переменным.

2. Ни y_i , ни y_j не подаются на вход другим гейтам и при этом хотя бы одна из переменных не является “ y_n для своего блока”. Такое невозможно. Доказательство практически повторяет доказательство во втором случае предыдущей теоремы.
3. Не умаляя общности, y_i не является “ y_n для своего блока” и не входит в другие гейты, а y_j является “ y_n для другого блока”. (При этом считаем, что в блоке с y_i есть хотя бы по 3 переменных, включая y_n) Это почти случаи 3-4 предыдущей теоремы. По тем же причинам g должен быть линейен. При этом очевидно, что g не может быть выходом ни одной из схем, так как в схеме, из которой y_n , выход y_n явно не зависит от y_i , а в схеме, где y_i , выходы нетривиально зависят еще от чего-то. Подставив вместо y_i y_n или $y_n \oplus 1$ (так, чтобы схема вычисляла H на $\frac{7}{8}$ оставшихся входов), исключаем как минимум 2 гейта. Заметим, что такая подстановка ничуть не портит утверждения 4 и в рамках одного блока представляет собой ничто иное как переименование переменной.
4. И y_i , и y_j являются “ y_n для своего блока”. Подставим вместо y_i y_j или $y_j \oplus 1$. Такое действие в худшем случае уничтожит один гейт, но нам это не важно. Мы можем вообще не учитывать этот исключенный гейт (на оценке это совершенно никак не отразится). При этом в блоке (или уже в блоках), где есть y_i , данная операция будет “воспринята” как переименование (если в том блоке уже есть y_j , то это равносильно подставлению в этом блоке “ y_n ” вместо чего-то, но этого чего-то изначально в этом блоке не было, поэтому нам это совершенно безразлично; аналогично если мы наоборот сначала подставили “ y_n ” вместо “ y_n ”, а потом “ y_n ” вместо “ y_i ”, то это равносильно подставлению “вместо y_i своего y_n ” и тоже исключает 2 гейта, так что все в порядке). Так что с точки зрения каждого блока мы ничего не потеряли, но при этом исключили ненужный топ-гейт.

Нетрудно видеть, что мы можем подставлять “хорошие” переменные до тех пор, пока в блоке не останется 2 переменные (если эти переменные “не свои”, то мы их не подставляем абы-как по случаю тривиализации это матрицы, а ждем, пока они подставятся другим путем. y_n , которой используется в других блоках в том же качестве при тривиализации блока не подставляется, пока живы другие блоки.) – тогда их можно подставить и забыть про этот отработанный блок. При этом необходимо отметить, что если одна и та же переменная

является “ y_n ” для одного блока (родного) и чем-то еще для другого, то при рассмотрении вышеуказанных случаев она считается “ y_n ” для своего родного блока. Таким образом, в каждом блоке получается по $n - 2$ “хороших” переменных и значит, $C_{7/8}(H) \geq m(2n - 4)$.

□

Замечание 1. Утверждение остается верным, если размерности блоков различны, как как приведенное доказательство совершенно не опирается на их одинаковость. Этот факт в дальнейшем пригодится при построении надежной в слабом смысле функции с секретом.

Теорема 4. p – произвольная функция от n . Если схема вычисляет H на более чем $\frac{1}{p(m)}$ доле входов, то ее сложность не менее $(2n - 4)(m - \log_{8/7} p(m))$.

Доказательство. ² Заметим, что H состоит из m отдельных блоков с непересекающимися множествами переменных X_i ; обозначим $h_i = H|_{X_i}$. Поскольку X_i не пересекаются, ошибки в вычислении функций h_i независимы. Следовательно, в матрице H есть не более $\log_{8/7} p(m)$ блоков, где схема C может себе позволить ошибиться на $\frac{1}{8}$ входов. На протяжении этого доказательства мы будем называть их “ужасными” блоками. Подставив вместо всех переменных, входящих в “ужасные блоки”, какие-нибудь значения, мы попадаем в условия утверждения 5 для $m \mapsto m - \log_{8/7} p(m)$.

□

Теорема 4 позволяет нам построить семейство слабо односторонних функций $\{f_n\}_{n=1}^{\infty}$ со сверхполиномиальными гарантиями надежности. Например, в терминах теоремы 4 можно в качестве n взять n^α при $\alpha < 1$, а в качестве m , соответственно, $n^{1-\alpha}$ (более строго $[n^\alpha]$ и $[n/[n^\alpha]]$). Тогда если схема вычисляет f_n^{-1} на более чем $(8/7)^{-\delta n^\beta}$ доле входов при $\delta > 0$ и $\beta < \alpha$, то размер этой схемы должен быть как минимум

$$(2n^\alpha - 4)(n^{1-\alpha} - \delta n^\beta) = 2n - 2\delta n^{\alpha+\beta} - 4n^{1-\alpha} + 4\delta n^\beta = 2n - o(n).$$

4.5 Семейство слабо односторонних функций со сколь угодно большой степенью обратной функции

Одно из принципиальных отличий нелинейных функций от линейных заключается в том, что обратная для линейной функции непременно

²Это доказательство идеологически повторяет доказательство леммы 9 из [HN08] с некоторыми поправками на нелинейность f_n^{-1}

является линейной, а обратная для нелинейной вовсе не обязана быть той же степени (под степенью функции здесь понимается максимальная степень компонентных функций). При незначительной модификации мы получаем из предыдущего примера семейство квадратичных слабо односторонних функций $\{f_n\}$, у которых степень f_n^{-1} стремится к бесконечности при $n \rightarrow \infty$.

$$\begin{aligned}
y_1 &= x_1 \oplus x_2 x_3 \\
y_2 &= x_2 \oplus x_3 x_4 \\
&\dots \\
y_k &= x_k \oplus x_{k+1} x_{k+2} \\
y_{k+1} &= (x_{k+1} \oplus x_{k+2}) x_n \oplus x_{k+2} \\
y_{k+2} &= (x_{k+1} \oplus x_{k+2}) x_n \oplus x_{n-1} \\
y_{k+3} &= x_{k+1} \oplus x_{k+3} \\
y_{k+4} &= x_{k+3} \oplus x_{k+4} \\
&\dots \\
y_{n-1} &= x_{n-2} \oplus x_{n-1} \\
y_n &= x_n,
\end{aligned}$$

где $k = o(n)$ и $k \xrightarrow{n \rightarrow \infty} \infty$.

Для того, чтобы получить f_n^{-1} , сложим все строки от $(k+1)$ -й до предпоследней.

$$y_{k+1} \oplus \dots \oplus y_{n-1} = x_{k+1} \oplus x_{k+2}$$

Далее, подставляя y_n вместо x_n , находим x_{k+2} и x_{n-1} . Остальные x_i -е при $i > k$ выражаются через x_{n-1} по цепочке и обратная функция имеет вид:

$$\begin{aligned}
x_n &= y_n \\
x_{k+2} &= (y_{k+1} \oplus \dots \oplus y_{n-1})y_n \oplus y_{k+1} \\
x_{n-1} &= (y_{k+1} \oplus \dots \oplus y_{n-1})y_n \oplus y_{k+2} \\
x_{n-2} &= (y_{k+1} \oplus \dots \oplus y_{n-1})y_n \oplus y_{k+2} \oplus y_{n-1} \\
x_{n-3} &= (y_{k+1} \oplus \dots \oplus y_{n-1})y_n \oplus y_{k+2} \oplus y_{n-1} \oplus y_{n-2} \\
&\dots \\
x_{k+3} &= (y_{k+1} \oplus \dots \oplus y_{n-1})y_n \oplus y_{k+2} \oplus y_{n-1} \oplus \dots \oplus y_{k+4} \\
x_{k+1} &= (y_{k+1} \oplus \dots \oplus y_{n-1})y_n \oplus y_{k+2} \oplus \dots \oplus y_{n-1} \\
x_k &= y_k \oplus x_{k+1}x_{k+2} = \\
&= y_k \oplus ((y_{k+1} \oplus \dots \oplus y_{n-1})y_n \oplus y_{k+2} \oplus \dots \oplus y_{n-1})((y_{k+1} \oplus \dots \oplus y_{n-1})y_n \oplus y_{k+1}) = \\
&= y_k \oplus y_{k+1}(y_{k+2} \oplus \dots \oplus y_{n-1}) \\
x_{k-1} &= y_{k-1} \oplus x_kx_{k+1} \\
&\dots \\
x_1 &= y_1 \oplus x_2x_3
\end{aligned}$$

Утверждение 6. f_n^{-1} имеет степень не менее $\lceil \frac{k}{2} \rceil + 1$.

Доказательство. $x_k = y_k + y_{k+1}(y_{k+2} + \dots + y_{n-1})$ имеет степень 2. Заметим, что для $i \leq k-2$ x_i обладает степенью как минимум на единицу большей, чем x_{i+2} ($x_i = y_i + y_{i+1}y_{i+2}$, x_{i+1} содержит слагаемое y_{i+1} , которого нет в x_{i+2} , поэтому степень $y_{i+1}y_{i+2}$ как минимум на 1 больше, чем степень x_{i+2}). В результате получаем $\deg(x_1) = 2 + \lceil \frac{k-1}{2} \rceil = \lceil \frac{k}{2} \rceil + 1$. $\square$

Теорема 5. Последовательность функций $\{f_n\}_{n=1}^{\infty}$ имеет порядок необратимости не менее 2.

Доказательство. Нетрудно видеть, что f_n считается за $2k + (n - k + 1) = n + k + 1$ гейт. У f_n^{-1} каждая из компонентных функций $x_{k+1}, \dots, x_{n-1}$ нетривиально зависит от $n - k$ переменных и все эти компонентные функции различны. Поэтому для вычисления f_n^{-1} требуется как минимум $(n - k - 1) + (n - k - 2) = 2n - 2k - 3$ гейта.

$$\lim_{n \rightarrow \infty} \frac{2n - 2k - 3}{n + k + 1} = 2, \text{ так как } k = o(n).$$

$\square$

Замечание 1. В этой конструкции почти все компонентные функции f_n^{-1} квадратичны. Можно увеличить k до $O(n)$, но это неминуемо приведет к уменьшению порядка необратимости.

Утверждение 7. При $k < \frac{n}{3} + g(n) \quad \forall g = o(n)$ последовательность функций $\{f_n\}_{n=1}^{\infty}$ имеет порядок необратимости строго больше 1.

Доказательство. Исходя из предыдущего доказательства, порядок необратимости $\{f_n\}_{n=1}^{\infty}$ больше 1, если

$$\lim_{n \rightarrow \infty} \frac{2n - 2k - 3}{n + k + 1} > 1 \Leftrightarrow \forall g = o(n) \quad 2n - 2k - 3 > n + k + 1 + g(n)$$

$$\Leftrightarrow \forall g = o(n) \quad n > 3k + g(n) \Leftrightarrow \forall g = o(n) \quad k < \frac{n}{3} + g(n)$$

□

4.6 Дальнейшие попытки улучшения константы.

Для ускорения перебора всевозможных кандидатов в слабо односторонние функции была написана небольшая компьютерная программа. В нее были заложены два алгоритма обращения квадратичных функций $f : B^n \rightarrow B^n$.

1. Алгоритм обращения “в лоб”. Вычисляет значения функции на всех входах. Если какие-то два значения совпали, говорит, что функция необратима. В противном случае последовательно восстанавливается обратная, исходя из предположения, что она является степенной. На первом шаге рассматривается вектор $X = (x_1, \dots, x_n)$ при $Y = (0, \dots, 0, 1, 0, \dots)$ (единица на i -м месте) для всех $i \in [1..n]$. Если $x_k = 1$, то одночлен y_i входит в x_k , если $x_k = 0$, то не входит. На втором шаге рассматриваются двучлены. И т.д.
2. Алгоритм обращения, работающий в предположении, что обратная функция тоже квадратична. Пусть прямая функция имеет вид: $y_k = \sum_{i,j=1, i \leq j}^n a_{ij} x_i x_j$, $k \in [1..n]$. Тогда обратная функция выглядит так:

$$x_k = \sum_{i,j=1, i \leq j}^n b_{ij} y_i y_j = \sum_{i,j=1, i \leq j}^n b_{ij} \left(\sum_{l=1, l \leq m}^n a_{lm} x_l x_m \right) \left(\sum_{p,r=1, p \leq r}^n a_{pr} x_p x_r \right),$$

где $k \in [1..n]$. Эти выражения преобразуются в систему линейных уравнений относительно b_{ij} , которые решаются методом Гаусса.

Программа имеет интерфейс для обращения произвольной квадратичной функции от небольшого количества переменных (до 10). Но основной ее вариант использования – это перебор определенных не очень больших множеств функций определенного

вида (от небольшого фиксированного количества переменных) на предмет проверки обратимости и сложности обратной (по довольно элементарным эвристикам, например, “хотя бы $n - 2$ выхода должны зависеть от хотя бы $n - 1$ входа”).

В результате использования программы был построен еще один кандидат в семейство слабо односторонних функций, но доказать про него что-либо известными методами не представляется возможным и предполагаемый порядок необратимости у него всего $\frac{4}{3}$. Однако сам факт того, что удалось что-то найти, говорит о возможной перспективности данного метода.

5 Надежная в слабом смысле функция с секретом.

В этом разделе я коротко опишу конструкцию надежной в слабом смысле функции с секретом, построенной на основе главной конструкции настоящей работы – слабо односторонней функции с порядком необратимости 2. Эта конструкция отличается от построенной Гиршом и Николенко тем, что в вычисляющих функциях $f^{-1}(pi)$ “ксорится” не с $f(m)$, а просто с m . В предлагаемой конструкции $c(n) = m(n) = (\alpha + 1)n$ и $pi(n) = ti(n) = n$, при этом ti является начальным числом генератора. α – это целое число, оптимальное значение которого будет позже определено. Входное сообщение m делится на 2 части: m_1 размера n и m_2 размера αn . К обеим частям при кодировании и декодировании применяются различные независимые друг от друга конструкции. Дадим формальное описание.

$$\begin{aligned} Key_n(s) &= (f_n(s), s), \\ Eval_n(pi, m_1, m_2) &= (f_n^{-1}(pi) \oplus m_1, f_{\alpha n}(m_2)), \\ Inv_n(ti, c_1, c_2) &= (f_n^{-1}(pi) \oplus c_1, f_{\alpha n}^{-1}(c_2)) = (ti \oplus c_1, f_{\alpha n}^{-1}(c_2)), \\ Adv_n(pi, c_1, c_2) &= (f_n^{-1}(pi) \oplus c_1, f_{\alpha n}^{-1}(c_2)), \end{aligned}$$

где Adv_n – это функция, которую должен вычислить взломщик, не знающий секрета, чтобы обратить данную конструкцию.

Утверждения, доказанные нами в предыдущем разделе, позволяют сформулировать следующее нижние и верхние оценки:

$$\begin{aligned} (Key_n) &\leq n + 1, \\ C(Eval_n) &\leq 2n - 2 + n + \alpha(n + 1) = 3n - 2 + \alpha(n + 1), \\ C(Inv_n) &\leq n + \alpha(2n - 2), \\ C_{7/8}(Adv_n) &\geq 2n - 4 + \alpha(2n - 4) \text{ (игнорируем } \oplus c_1). \end{aligned}$$

Чтобы порядок надежности построенного семейства был оптимален, нам необходимо подобрать значение α , максимизирующее

$$\begin{aligned} \liminf_{i \rightarrow \infty} \min \left\{ \frac{C_{7/8}(Adv_n)}{C(Key_n)}, \frac{C_{7/8}(Adv_n)}{C(Eval_n)}, \frac{C_{7/8}(Adv_n)}{C(Inv_n)} \right\} = \\ \min \left\{ \frac{2 + 2\alpha}{1}, \frac{2 + 2\alpha}{3 + \alpha}, \frac{2 + 2\alpha}{1 + 2\alpha} \right\} = \\ \min \left\{ \frac{2 + 2\alpha}{3 + \alpha}, \frac{2 + 2\alpha}{1 + 2\alpha} \right\}. \end{aligned}$$

В целях экономии места не буду приводить здесь выкладки, связанные с поиском корней квадратного уравнения и прочими техническими подробностями нахождения минимума, а сразу напишу, что оптимальное значение порядка надежности, равное $\frac{6}{5}$, достигается при $\alpha = 2$.

Замечание 1. Предполагается, что эту константу можно улучшить до $\frac{7}{5}$, если аккуратно доказать, что засчет “ $\oplus c_1$ ” сложность обращения без “секрета” на самом деле больше.

Замечание 2. Руководствуясь теоремами из предыдущего раздела, можно построить на базе приведенного семейства семейство функций с секретом со сверхполиномиальными гарантиями надежности.

6 Заключение.

6.1 Результаты.

1. Построено семейство нелинейных слабо односторонних функций с порядком необратимости $\frac{6}{5}$.
2. Построено семейство нелинейных слабо односторонних функций с порядком необратимости 2. Для этого семейства доказано, что схема, которая обращает f_n^{-1} на более чем $\frac{7}{8}$ входов, содержит как минимум $2n - 4$ гейта, что всего на 1 гейт меньше, чем схемная сложность f_n^{-1} .
3. На базе этого семейства построено семейство с порядком необратимости 2 и со сверхполиномиальными гарантиями надежности против более слабых соперников. Иными словами, взломщик, располагающий немного меньшим (по сравнению с длиной входа) количеством гейтов сможет обратить нашу функцию лишь на сверхполиномиальной доле входов.
4. На базе этого семейства построено семейство слабо односторонних функций с порядком необратимости 2 такое, что степень обратной функции неограниченно растет с ростом n .

Стоит признать, что особой пользы в этом примере от неограниченного роста степени обратной функции нет. Напротив, чем быстрее этот рост, тем быстрее вычисляется обратная функция. Однако чем выше степень функции, тем больше максимально возможное количество гейтов в оптимальной схеме для этой функции. И тот факт, что обратной для квадратичной функции может быть функция сколь угодно большой степени, вселяет некоторые надежды на то, что существуют гораздо более удачные примеры.

5. На базе этого семейства построено семейство функций с секретом с порядком надежности $\frac{6}{5}$ (на основе которого тоже можно построить семейство со сверхполиномиальными гарантиями надежности).

6.2 Направления дальнейших исследований.

В настоящей работе представлены первые конструкции нелинейных слабо односторонних функций. Возможные направления дальнейших исследований.

1. Улучшение константы. Поиск новых семейств нелинейных слабо односторонних функций, принципиально отличающихся от приведенных в этой работе. В качестве одного из методов поиска предлагается использование компьютерной программы для автоматизации перебора и отсева заведомо неинтересных случаев.
2. Конструирование других надежных в слабом смысле криптографических примитивов на базе нелинейных функций.
3. Усовершенствование имеющихся и изобретение новых методов доказательства нижних оценок.

Список литературы

- [Hil92] Alain P. Hiltgen. Constructions of freely-one-way families of permutations. In Proc. of AsiaCrypt '92, pages 422-434, 1992.
- [HN08] Edward A. Hirsch, Sergey I. Nikolenko. A feebly trapdoor function. PDMI preprint 16/2008.
- [LS73] E. A. Lamagna and J. E. Savage. On the logical complexity of symmetric switching functions in monotone and complete bases. Technical report, Brown University, Rhode Island, jul 1973.
- [Sav76] John E. Savage. The Complexity of Computing. Wiley, New York, 1976.
- [Mas96] James L. Massey. The Difficulty with Difficulty. A Guide to the Transparancies and Transparancies from EUROCRYPT '96 IACR. Lecture.