

## **ПРЕПРИНТЫ ПОМИ РАН**

### **ГЛАВНЫЙ РЕДАКТОР**

**С.В. Кисляков**

### **РЕДКОЛЛЕГИЯ**

**В.М.Бабич, Н.А.Вавилов, А.М.Вершик, М.А.Всемирнов, А.И.Генералов, И.А.Ибрагимов,  
Л.Ю.Колотилина, Б.Б.Лурье, Ю.В.Матиясевич, Н.Ю.Нецветаев, С.И.Репин, Г.А.Серегин**

**Учредитель: Санкт-Петербургское отделение Математического института  
им. В. А. Стеклова Российской академии наук**

**Свидетельство о регистрации средства массовой информации: ЭЛ №ФС 77-33560 от 16  
октября 2008 г. Выдано Федеральной службой по надзору в сфере связи и массовых  
коммуникаций**

**Контактные данные: 191023, г. Санкт-Петербург, наб. реки Фонтанки, дом 27**

**телефоны: (812)312-40-58; (812) 571-57-54**

**e-mail: [admin@pdmi.ras.ru](mailto:admin@pdmi.ras.ru)**

**<http://www.pdmi.ras.ru/preprint/>**

**Заведующая информационно-издательским сектором Симонова В.Н**

# НЕЛИНЕЙНЫЕ НАДЕЖНЫЕ В СЛАБОМ СМЫСЛЕ КРИПТОГРАФИЧЕСКИЕ ПРИМИТИВЫ<sup>1</sup>

О. Ю. Меланич

Санкт-Петербургское отделение  
Математического института им. В. А. Стеклова  
Российской академии наук

<http://logic.pdmi.ras.ru/~melanich>

17 декабря 2009

## Аннотация

В классической криптографии односторонние функции являются базовыми примитивами для протоколов согласования ключа и цифровой подписи, а функции с секретом служат основой для криптосистем с открытым ключом. Как известно, не существует никаких доказательств того, что та или иная функция (искусственно построенная или используемая в практической криптографии) является односторонней функцией или функцией с секретом. Однако существуют конструкции *функций, односторонних в слабом смысле, и надежных в слабом смысле функций с секретом*, сложность обращения которых *доказуемо* больше, чем сложность вычисления, но пока лишь в константное число раз.

В 1992 году Ален Хильтген [Hil92] построил функцию, обратить которую вдвое сложнее, чем вычислить. В 2009 году Э. А. Гирш и С. И. Николенко [HN09] предложили конструкцию *надежной в слабом смысле функции с секретом*, основанную на функции Хильтгена. Обе вышеупомянутые конструкции линейны, что мало перспективно (сложность взломщика не может быть более чем квадратом сложности честных участников протокола). Автор продолжает исследования Хильтгена, Гирша и Николенко и конструирует первые *нелинейные* надежные в слабом смысле криптографические примитивы: одностороннюю в слабом смысле функцию и основанную на ней функцию с секретом.

---

<sup>1</sup>НИР проведена в рамках реализации ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 годы, госконтракт П265 от 23.07.2009. Частично поддержано грантом РФФИ 08-01-00640-а.

ПРЕПРИНТЫ  
Санкт-Петербургского отделения  
Математического института им. В. А. Стеклова  
Российской академии наук

PREPRINTS  
of the St. Petersburg Department of Steklov Institute of Mathematics

---

ГЛАВНЫЙ РЕДАКТОР  
С. В. Кисляков

РЕДКОЛЛЕГИЯ  
В. М. Бабич, Н. А. Вавилов, А. М. Вершик, М. А. Всемиров, А. И. Генералов, И. А. Ибрагимов,  
А. А. Иванов, Л. Ю. Колотилина, В. Н. Кублановская, Г. В. Кузьмина, П. П. Кулиш, Б. Б. Лурье,  
Ю. В. Матиясевич, Н. Ю. Нецветаев, С. И. Репин, Г. А. Серегин, В. Н. Судаков, О. М. Фоменко

# 1 Введение

В классической криптографии односторонние функции являются базовыми примитивами для протоколов согласования ключа и цифровой подписи, а функции с секретом служат основой для криптосистем с открытым ключом. Как известно, до сих пор не существует никаких доказательств того, что та или иная функция (искусственно построенная или используемая в практической криптографии) является односторонней функцией или функцией с секретом. Поскольку никто пока не умеет доказывать сверхполиномиальную разницу между сложностями честных участников протокола и сложностью взломщика, то логично попробовать для начала доказать *хоть какую-нибудь* разницу.

В 1992 году Ален Хильтген [Hil92] построил линейную функцию, обратить которую вдвое сложнее, чем вычислить. В 2009 году Э. А. Гирш и С. И. Николенко [HN09] предложили конструкцию *надежной в слабом смысле функции с секретом* с порядком надежности  $\frac{25}{22}$ , основанную на функции Хильтгена. В качестве модели вычисления в обеих работах использовались булевские схемы с произвольными бинарными гейтами.

Автор продолжает исследования Хильтгена, Гирша и Николенко. Поскольку сложность любой линейной функции от  $n$  переменных не превосходит  $n^2$  (а обратная к линейной тоже линейна), искать среди них кандидаты в односторонние функции бесперспективно. Поэтому данная работа посвящена именно нелинейным криптографическим примитивам, надежным в слабом смысле.

В разделе 2 даются базовые определения. В разделе 3 приводится краткое описание двух методов доказательства нижних оценок схемной сложности функций из  $\{0,1\}^n$  в  $\{0,1\}^m$ , которые будут использованы в настоящей работе. Раздел 4 содержит описание основной конструкции (нелинейной односторонней в слабом смысле функции), доказательства оценок ее сложности в худшем и в среднем случае, а также способ усовершенствования данной конструкции, позволяющий получить более сильные гарантии надежности против более слабых противников. В разделе 5 на базе основной конструкции строится надежная в слабом смысле функция с секретом. Раздел 6 включает в себя итоги данной работы и возможные направления дальнейших исследований.

## 2 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), либо имеет два входящих ребра (такие вершины называются гейтами). Каждый гейт помечен бинарной булевской 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 лишнего гейта-отрицаний). Также выходом может быть вход или отрицание входа.

Схема с  $n$  входами и  $m$  выходами естественным образом вычисляет функцию из  $B_{n,m}$ .

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

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

где  $C(c)$  – размер схемы  $c$ .

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.

А. Хильтген [Hil92] ввел для каждой обратимой (инъективной) функции  $f_n \in B_{n,m}$  понятие *меры сложности в слабом смысле* (measure of feeble one-wayness)

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

**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.

Э. А. Гирш и С. И. Николенко [HN09] ввели следующую систему определений для 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. Длина входа функции обозначается через  $m(n)$ , через  $c(n)$  – длина ее выхода, а через  $pi(n)$  и  $ti(n)$  – длина 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 определении успешного обращения вместо  $\frac{7}{8}$  используется константа  $\frac{3}{4}$ . Но это не имеет принципиального значения, так как предлагаемую в настоящей работе конструкцию надежной в слабом смысле функции с секретом можно усовершенствовать так, чтобы противник, имеющий немного меньшее количество гейтов, чем необходимое для успешного обращения, смог обратить ее только на экспоненциально малой доле входов.

**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  $n$ ,

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

В следующих разделах будет построена нелинейная односторонняя в слабом смысле функция (т.е. семейство функций, являющееся слабо односторонним) порядка 2 и основанная на ней надежная в слабом смысле функция с секретом (т.е. семейство кандидатов в функции с секретом с порядком надежности  $> 1$ ).

## 3 Методы доказательства нижних оценок схемной сложности

### 3.1 Оценки Ламаньи и Севиджа

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

**Теорема 1** ([LS73,Sav76]; [Hil92, Теоремы 3 и 4]; [HN09, 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 ни одна из них не равна отрицанию другой<sup>1</sup>, и для каждой из них  $C(f^{(i)}) \geq c > 1$ , то  $C(f) \geq c + m - 1$ .

В данной работе с помощью этих оценок будет доказано, что базовая конструкция является односторонней функцией порядка 2, а все остальные утверждения будут доказаны *методом исключения гейтов*.

### 3.2 Исключение гейтов

Метод *исключения гейтов* (*gate elimination*) позволяет доказывать более сильные результаты, однако более чем линейных оценок от него ожидать сложно. С его помощью было доказано большинство нижних оценок на размеры схем произвольного вида [Weg87].

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 константы вместо любой из переменных он станет унарным. Поэтому иногда бывает полезно подставлять вместо переменной не константу, а какую-нибудь функцию. Пусть, например, у нас есть линейный гейт  $g$  со входами  $x$  и  $y$ . Переменная  $x$  больше никуда не входит, а хочется одной подстановкой именно этой переменной исключить как минимум два гейта. Тогда можно подставить вместо  $x$  функцию  $Id(y)$  или  $NOT(y)$  (этот прием будет использован в настоящей работе<sup>2</sup>). Количество исключенных гейтов дает нижнюю оценку на схемную сложность  $f$ .

## 4 Семейство слабо односторонних функций порядка 2

### 4.1 Основная конструкция

Этот пример был получен путем объединения линейной функции Хильтгена с порядком необратимости  $\frac{3}{2}$  [Hil92] с первой вычислительно асимметричной функцией от 4 переменных, представленной на слайдах Мессии ([Mas96], слайд 18).

<sup>1</sup>Условия  $f^{(i)} \neq NOT(f^{(j)})$  у Ламаньи и Севиджа не было, но в нашем случае оно необходимо, так как в определении булевой схемы допускается, что выходом может быть не только гейт, но и его отрицание.

<sup>2</sup>Примеры использования данного приема можно также найти в [Weg87].

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  $x_k$  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.** Семейство функций  $\{f_n\}_{n=1}^{\infty}$  является слабо односторонним порядка 2.

**Доказательство.** Нетрудно видеть, что  $f_n$  вычисляется 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<sup>3</sup>. 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.

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

Устремляя  $n$  к бесконечности, получаем требуемое.

□

## 4.2 Сложность в среднем случае

В криптографии недостаточно, чтобы конструкцию было трудно взломать лишь иногда, – важно, чтобы это было так с вероятностью, близкой к 1. Мы предъявим конструкцию, для которой противник,

<sup>3</sup>Так как  $f_n$  обратима, к  $f_n$  и  $f_n^{-1}$  применима теорема 1.

обладающий немного меньшим количеством гейтов, чем строго необходимо для полного обращения, сможет обратить нашу функцию лишь на незначительной доле входов. Нетрудно видеть, что предложенная выше конструкция является совершенно ненадежной в данном смысле. Действительно, линейная часть  $f_n^{-1}$  совпадает с  $f_n^{-1}$  на  $\frac{3}{4}$  входов (когда  $x_n = 0$  и когда выражение в скобках равно 0), а вычисляется всего  $n - 3$  гейтами. Однако в следующем разделе будет показано, как модифицировать наше семейство для получения гораздо более сильных гарантий надежности. Для начала докажем, что построенное семейство обладает хоть какой-то надежностью в вышеупомянутом смысле: схема, обращающая  $f_n$  на более чем  $\frac{7}{8}$  ее входов, содержит хотя бы  $2n - 4$  гейта. Прежде чем доказывать этот факт, докажем одну подготовительную лемму.

**Лемма 1.** *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  $\forall k \in [1..l] a_{i_k} \in \{0, 1, y_n, y_n \oplus 1\}$  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.** Вначале заметим, что для  $i \neq n$

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

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

Будем доказывать первую часть утверждения 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. Противоречие.

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  $x_k|_{y_n=0} = y_i \oplus \dots$ , 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 такое  $k$ , что выход  $x_k = (y_j \oplus \dots) y_n \oplus y_j \oplus \dots$  (для всех  $j \neq 2$  подходит  $k = 1$ , для  $j = 2$  подходит  $k = 2$ ). 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. □

Через  $C_\delta(f)$  будем обозначать минимальный размер схемы, которая вычисляет  $f$  на доле входов, превосходящей  $\delta$ .

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

**Доказательство.** Рассмотрим оптимальную схему, вычисляющую  $f_n^{-1}$  на более чем  $\frac{7}{8}$  входов. Будем последовательно подставлять вместо некоторых переменных (кроме  $y_n$ ) значения из  $\{0, 1, y_n, y_n \oplus 1\}$  таким образом, чтобы после каждой подстановки исключать как минимум 2 гейта (далее будем называть такие переменные “хорошими”). Следующее утверждение неформально говорит о том, что, пока у нас остаются хотя бы 3 переменные, одна из которых –  $y_n$ , мы можем делать “хорошие” подстановки.

**Утверждение 1.** 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  $\forall k \in [1..l]$   $a_{i_k} \in \{0, 1, y_n, y_n \oplus 1\}$  на более чем  $\frac{7}{8}$  входов, в которой каждый гейт нетривиально зависит от обоих своих входов, можно подставить вместо одной из переменных, отличной от  $y_n$ , значение из  $\{0, 1, y_n, y_n \oplus 1\}$  так, чтобы при этом исключилось как минимум 2 гейта и чтобы полученная схема совпадала с  $f_n^{-1}$  на более чем  $\frac{7}{8}$  оставшихся входов.

**Доказательство.** Для краткости вместо  $f_n^{-1}|_{y_{i_1}=a_1, \dots, y_{i_l}=a_l}$  будем писать  $f_n^{-1}$ , а функцию, которую схема вычисляет на самом деле, обозначим через  $h$ . Пусть  $g$  – гейт, входы в который ведут из вершин схемы  $y_i$  и  $y_j$ . По лемме 1 такой гейт существует. 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.
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 лемме 1). 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  $y_j \notin Z$ . Так как в нашей 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.

(b)  $h_k$  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,  $j = n$ ,  $y_i$  не подается на вход другим гейтам, и  $g$  нелинеен. Покажем, что такое невозможно. Действительно, иначе при подходящем значении  $y_n$  ни один из выходов не зависил 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,  $j = n$ ,  $y_i$  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 (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). Значит,  $g$  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.

□

Поскольку наша схема оптимальна, каждый гейт в ней и в ее сужениях нетривиально зависит от обоих входов. Значит, и она, и все ее сужения, полученные описанными в утверждении 1 подстановками не более чем  $n - 3$  переменных, удовлетворяют условию утверждения 1. Таким образом, мы можем последовательно подставить в нашу схему  $n - 2$  “хорошие” переменные, исключив при этом как минимум  $2n - 4$  гейта.

□

**Замечание 2.** Как было замечено Григорием Ярославцевым, на самом деле можно доказать, что  $S_{3/4}(f_n^{-1}) \geq 2n - 4$ . Для этого достаточно в случае 2а аккуратно рассмотреть случаи линейности и нелинейности гейта  $g$ . И все последующие нижние оценки на схемную сложность останутся верными, если заменить  $\frac{7}{8}$  на  $\frac{3}{4}$  (чтобы в этом убедиться, потребуется более аккуратно рассмотреть еще пару случаев в приведенных ниже доказательствах).

### 4.3 Более сильные гарантии надежности

В предыдущем разделе было показано, что противник, использующий 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 против более слабых противников.

Определим функцию  $H : B^{mn} \rightarrow B^{mn}$  следующим образом: область определения разбивается последовательно на  $t$  блоков по  $n$  переменных и к каждому такому блоку применяется  $f_n^{-1}$ . Обозначим за  $Y_n$  множество переменных, являющихся последними в своем блоке. Сформулируем для  $H$  утверждение, аналогичное лемме 1.

**Лемма 2.** В схеме, вычисляющей  $H|_{y_{i_1}=a_1, \dots, y_{i_l}=a_l, y_{j_1}=a_{l+1}, \dots, y_{j_m}=a_{l+m}}$  или  $H|_{y_{i_1}=a_1, \dots, y_{i_l}=a_l, y_{j_1}=a_{l+1}, \dots, y_{j_m}=a_{l+m}, y_{i_n}=c}$ , где

1.  $l \leq n - 3$ ,
2.  $y_{i_1}, \dots, y_{i_l}, y_{i_n}$  из одного блока,
3.  $\{y_{i_1}, \dots, y_{i_l}\} \cap Y_n = \emptyset, y_{i_n} \in Y_n$   
(Менее формально: в некотором блоке остались как минимум 2 переменные не из  $Y_n$ ),
4.  $y_{j_1}, \dots, y_{j_m}$  принадлежат другим блокам,
5.  $\forall k \in [1..l + m] \ a_k \in \{0, 1\} \cup Y_n \cup \{y \oplus 1 | y \in Y_n\}$ ,
6.  $c \in Y_n \setminus y_{i_n} \cup \{y \oplus 1 | y \in Y_n \setminus y_{i_n}\}$ ,

на более чем  $\frac{3}{4}$  входов, ни одна из переменных данного блока, кроме, возможно,  $y_{i_n}$ , не является выходом схемы и входит хотя бы в один гейт.

**Доказательство.** Заметим, что подстановка вместо переменной из нашего блока переменной из другого блока выглядит как переименование. Если вместо  $y_{i_n}$  и  $y_{i_k}$  подставлена одна и та же переменная, то это выглядит как подстановка  $y_{i_n}$  вместо  $y_{i_k}$ . Если одна и та же переменная подставлена вместо нескольких переменных нашего блока, отличных от  $y_{i_n}$ , то это выглядит как замена этих переменных в скобке на что-то линейное, не включающее  $y_{i_n}$  (или то, на что его заменили) и нетронутые переменные из нашего блока, и замена этих переменных в линейной части на что-то такого же вида. Нетрудно видеть, что доказательство, приведенное для леммы 1, при таких заменах отлично проходит. Очевидно, что  $y_{i_k}$  не может быть выходом  $h_s$  в другом блоке, так как  $x_s$  не зависит от  $y_{i_k}$ .

□

**Лемма 3.**  $C(H) \geq m(2n - 4)$  и, более того,  $C_{7/8}(H) \geq m(2n - 4)$ .

**Доказательство.** Проводим индуктивное рассуждение, аналогичное приведенному в теореме 3. Когда в блоке будет оставаться только одна переменная не из  $Y_n$ , мы будем подставлять вместо нее значение из  $\{0, 1\}$  так, чтобы полученная в результате схема по-прежнему вычисляла  $H$  на более чем  $\frac{7}{8}$  оставшихся входов. Поэтому далее считаем, что в рассматриваемых блоках либо нет переменных не из  $Y_n$ , либо их хотя бы 2.

**Утверждение 2.** В схеме, вычисляющей функцию  $H$ , в которой вместо некоторых переменных не из  $Y_n$  подставлены значения из  $\{0, 1\} \cup Y_n \cup \{y \oplus 1 | y \in Y_n\}$ , вместо некоторых переменных из  $Y_n$  подставлены значения из  $Y_n \cup \{y \oplus 1 | y \in Y_n\}$  и при этом хотя бы в одном блоке осталось хотя бы 2 переменные  $\notin Y_n$ , на более чем  $\frac{7}{8}$  входов, в которой каждый гейт нетривиально зависит от обоих своих входов, можно либо подставить вместо одной из переменных не из  $Y_n$  значение из  $\{0, 1\} \cup Y_n \cup \{y \oplus 1 | y \in Y_n\}$  так, чтобы при этом исключилось как минимум 2 гейта, либо подставить вместо  $z \in Y_n$  значение из  $Y_n \setminus z \cup \{y \oplus 1 | y \in Y_n \setminus z\}$ . И то и другое можно сделать так, чтобы полученная схема совпадала с  $H$  на более чем  $\frac{7}{8}$  оставшихся входов.

**Доказательство.** Пусть  $g$  – гейт, входы в который ведут из вершин схемы  $y_i$  и  $y_j$ . По лемме 2 такой гейт существует. Функцию, которую схема вычисляет на самом деле, обозначим через  $h$ . Заметим, что все случаи, которые рассматривались в утверждении 1, остаются верными в общем контексте, если переменные, входящие в  $g$ , принадлежат одному блоку. Рассмотрим случаи принадлежности входов  $g$  к разным блокам. Не умаляя общности, будем считать, что  $y_i$  входит в первый блок ( $i \in [1..n]$ ), а  $y_j$  – во второй ( $j \in [n + 1..2n]$ ).

1.  $y_i$  входит еще в один гейт, и при этом  $i \neq n$ . 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  $i \neq n$  и  $j \neq 2n$ . Покажем, что такое невозможно. По лемме 2  $y_i$  и  $y_j$  не являются выходами (так как в обоих блоках есть как минимум 2 переменные не из  $Y_n$ ), поэтому доказательство практически повторяет доказательство в случае 2 утверждения 1 (только в нашем случае  $x_k$  вообще не зависит от  $y_j$ ).

3. Не умаляя общности,  $i \neq n$  и  $y_i$  не входит в другие гейты,  $j = 2n$ , и  $g$  *нелинейна*. Покажем, что такое невозможно. Действительно, иначе при подходящем значении  $y_j$  ни один из выходов не зависил бы от  $y_i$ . По построению  $f_n^{-1}$  найдется выход  $x_k|_{y_n=0} = y_i \oplus \dots$ . Тогда

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

а

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

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

4. Не умаляя общности,  $i \neq n$  и  $y_i$  не входит в другие гейты,  $j = 2n$ , и  $g$  *линейна*. Покажем, что  $g$  не может быть выходом схемы. Пусть  $g$  – это выход схемы  $h_k$ . Возможны следующие случаи.

- (а)  $k < n$ . По условию в первом блоке помимо  $y_i$  и  $y_n$  осталась еще хотя бы одна переменная  $y_l$ . По построению  $f_n^{-1}$  существует значение  $y_n$ , при котором  $x_k = y_l \oplus \dots$ . Тогда

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

а

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

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

- (б)  $k \geq n$ . Тогда  $x_k|_{y_i=0} = x_k|_{y_i=1}$ , а  $h_k|_{y_i=0} \neq h_k|_{y_i=1}$ . Поэтому  $h$  отличается от  $H$  хотя бы на  $\frac{1}{2}$  входов. Противоречие.

Значит, у  $g$  есть потомки. Сделаем ту из подстановок  $y_i = y_j$  или  $y_i = y_j \oplus 1$ , при которой  $h$  будет по-прежнему совпадать с  $H$  на более чем  $\frac{7}{8}$  входов. Этим мы исключаем и сам гейт  $g$ , и его потомков, то есть как минимум 2 гейта.

5.  $i = n$  и  $j = 2n$ . Подставим вместо  $y_i$   $y_j$  или  $y_j \oplus 1$  (так, чтобы полученная схема совпадала с  $H$  на более чем  $\frac{7}{8}$  оставшихся входов).

На каждом шаге мы либо подставляем “хорошую” переменную, либо подставляем переменную из  $Y_n$ . При этом пока существует блок, в котором есть хотя бы 2 переменные не из  $Y_n$ , полученные описанным в утверждении 2 способом схемы удовлетворяют условию утверждения 2. Таким образом, в каждом блоке получается по  $n - 2$  “хорошие” переменные и, значит,  $C_{7/8}(H) \geq m(2n - 4)$ .

□

**Замечание 3.** Лемма остается верной, если размерности  $n_i$  блоков различны, так как приведенное доказательство совершенно не опирается на их одинаковость:

$$C_{7/8}(H) \geq \sum_{i=1}^m (2n_i - 4).$$

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

**Доказательство.** 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. Подставив вместо всех переменных, входящих в эти блоки, какие-нибудь значения, мы попадаем в условия леммы 3 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  $n^\alpha$  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  $\beta < 1 - \alpha$ , то размер этой схемы должен быть как минимум

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

## 5 Надежная в слабом смысле функция с секретом

На основе нашей базовой конструкции односторонней функции почти аналогичным описанному в [HN09] методом может быть построена надежная в слабом смысле функция с секретом (т.е. семейство кандидатов в функцию с секретом с порядком надежности  $> 1$ ). Опишем это построение в терминах определения 4:  $c(n) = m(n) = (\alpha + 1)n$  и  $pi(n) = ti(n) = n$ , при этом  $ti$  является начальным числом генератора,  $\alpha$  – это целое число, оптимальное значение которого будет далее определено. Входное сообщение  $m$  делится на 2 части:  $m_1$  размера  $n$  и  $m_2$  размера  $\alpha n$ . К обеим частям при кодировании и декодировании применяются различные независимые друг от друга конструкции. Вот 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.

Для того, чтобы доказать нажную оценку для  $Adv_n$ , придется немного переформулировать и усложнить утверждения, доказанные в предыдущем разделе.

Определим функцию  $G : B^{2nm_1 + \alpha nm_2} \rightarrow B^{nm_1 + \alpha nm_2}$  следующим образом: область определения состоит из  $m_1$  блоков по  $2n$  переменных (к каждому такому блоку применяется  $f_n^{-1} \oplus c$ , где  $c$  – это  $n$  последних переменных блока, а  $f_n^{-1}$  применяется к первым  $n$  переменным) и  $m_2$  блоков по  $\alpha n$  переменных (к каждому такому блоку применяется  $f_{\alpha n}^{-1}$ ). ( $Adv_n$  – это  $G$  для  $m_1 = m_2 = 1$ .)

Обозначим за  $Y_n$  множество переменных, каждая из которых либо принадлежит блоку из  $2n$  переменных и имеет в нем номер  $n$ , либо принадлежит блоку из  $\alpha n$  переменных и является в нем последней. Обозначим за  $C$  множество переменных, каждая из которых принадлежит блоку из  $2n$  переменных и имеет в нем номер, строго больший, чем  $n$ . Элементы этого множества будем обозначать  $c_i$ , а все остальные переменные –  $y_i$ . Множество элементов  $i$ -го блока будем обозначать  $X_i$ .

**Лемма 4.** В схеме, вычисляющей  $G|_{y_{i_1}=a_1, \dots, y_{i_l}=a_l, c_{p_1}=d_1, \dots, c_{p_s}=d_s, y_{j_1}=a_{l+1}, \dots, y_{j_m}=a_{l+m}}$  или  $G|_{y_{i_1}=a_1, \dots, y_{i_l}=a_l, c_{p_1}=d_1, \dots, c_{p_s}=d_s, y_{j_1}=a_{l+1}, \dots, y_{j_m}=a_{l+m}, y_{in}=c}$ , где

1.  $l \leq n - 3$ ,
2.  $y_{i_1}, \dots, y_{i_l}, y_{i_n}$  из одного блока  $X_r$ ,
3.  $\{y_{i_1}, \dots, y_{i_l}\} \cap Y_n = \emptyset$ ,  $y_{i_n} \in Y_n$   
(Менее формально: в блоке  $X_r$  остались как минимум 2 переменные не из  $Y_n \cup C$ ),
4.  $y_{j_1}, \dots, y_{j_m}$  принадлежат другим блокам
5.  $\forall k \in [1..l+m] \ a_k \in \{0, 1\} \cup Y_n \cup \{y \oplus 1 | y \in Y_n\}$   
(при этом  $\forall t$  вместо последней переменной из  $X_t \setminus C \setminus Y_n$  может также быть подставлено значение из  $X_t \cap C \cup \{c \oplus 1 | c \in X_t \cap C\}$ ),
6.  $c \in Y_n \setminus y_{i_n} \cup \{y \oplus 1 | y \in Y_n \setminus y_{i_n}\}$ ,

7.  $s \geq 0, \forall k \in [1..s] \ d_k \in \{0, 1\}$ ,

на более чем  $\frac{3}{4}$  входов:

1. Ни одна из переменных  $X_r \setminus C$ , кроме, возможно,  $y_{i_n}$ , не является выходом схемы и входит хотя бы в один гейт.
2. При  $l \leq n - 2$ , все переменные из  $C \cap X_r$  не являются выходами и входят хотя бы в один гейт.
3. Если  $l = n - 2$ , а вместо последней переменной из  $X_r \setminus C \setminus Y_n$  подставлено значение из  $X_r \cap C \cup \{c \oplus 1 | c \in X_r \cap C\}$ , то все переменные из  $C \cap X_r$  не являются выходами и входят хотя бы в один гейт.

**Доказательство.**

1. Уже доказано (Лемма 2; наличие в некоторых выходах дополнительного элемента в линейной части, очевидно, не портит приведенных рассуждений).
2. Пусть  $c_k$  является выходом  $h_l$ . Если  $x_l$  не зависит от  $c_k$ , то, очевидно, что  $h$  отличается от  $G$  на половине входов. В противном случае, существует  $y_s : x_l = (y_s \oplus \dots)y_p \oplus c_k \oplus \dots$ . Тогда при одном из значений  $y_p$   $x_l = y_s \oplus c_k \oplus \dots$  и  $h$  отличается от  $G$  на четверти входов. Противоречие. Пусть  $c_k$  не является выходом и не входит ни в один гейт. Тогда  $h$  вообще не зависит от  $c_k$ . Существует выход  $x_l = c_k \oplus \dots$ . Значит,  $h$  и  $G$  отличаются хотя бы на половине входов. Противоречие.
3. Пусть  $c_k$  является выходом  $h_l$ . Если  $x_l$  не зависит от  $c_k$ , то, очевидно, что  $h$  отличается от  $G$  на половине входов. В противном случае возможны 3 варианта:

(a)  $x_l = (c_k \oplus \dots)y_p \oplus c_k \oplus \dots$  Тогда

$$h_l(y_p = 1, c_k = 0, \dots) \neq h_k(y_p = 1, c_k = 1, \dots),$$

а

$$x_k(y_p = 1, c_k = 0, \dots) = x_k(y_p = 1, c_k = 1, \dots),$$

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

(b)  $x_l = (c_k \oplus \dots)y_p \oplus \bigoplus_{z \in Z} z \oplus a, Z \subseteq X_r \setminus \{c_k\}, a \in \{0, 1\}$ . Тогда

$$h_l(y_p = 0, c_k = 0, \dots) \neq h_k(y_p = 0, c_k = 1, \dots),$$

а

$$x_k(y_p = 0, c_k = 0, \dots) = x_k(y_p = 0, c_k = 1, \dots),$$

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

(c)  $x_l = (c_l \oplus \dots)y_p \oplus c_k \oplus \dots$ . Этот случай разобран в предыдущем пункте.

Пусть  $c_k$  не является выходом и не входит ни в один гейт. Тогда существует выход  $x_l$ , равный либо  $c_k \oplus \dots$ , либо  $(c_k \oplus \dots)y_p \oplus c_k \oplus \dots$ . Значит,  $h$  и  $G$  отличаются хотя бы либо на половине, либо на четверти входов соответственно. Противоречие.

□

**Теорема 5.**  $C_{7/8}(G) \geq m_1(3n - 4) + m_2(2\alpha n - 4)$ .

**Доказательство.** Проводим индуктивное рассуждение, аналогичное приведенному в лемме 3 и теореме

3. Когда в блоке будет оставаться только одна переменная  $y_i \notin Y_n \cup C$ , мы будем делать следующее:

1. Если в блоке не осталось переменных из  $C$ , подставим вместо  $y_i$  значение из  $\{0, 1\}$  так, чтобы полученная в результате схема по-прежнему вычисляла  $G$  на более чем  $\frac{7}{8}$  оставшихся входов.

2. Если в блоке есть  $c \in C$ , то подставим вместо  $y_i$  значение из  $\{c, c \oplus 1\}$  так, чтобы полученная в результате схема по-прежнему вычисляла  $G$  на более чем  $\frac{7}{8}$  оставшихся входов.

Поэтому далее считаем, что в рассматриваемых блоках либо нет переменных не из  $Y_n \cup C$ , либо их хотя бы 2.

**Утверждение 3.** В схеме, вычисляющей функцию  $G$ , в которой вместо некоторых переменных не из  $Y_n \cup C$  подставлены значения из  $\{0, 1\} \cup Y_n \cup \{y \oplus 1 | y \in Y_n\}$ , вместо некоторых переменных из  $Y_n$  подставлены значения из  $Y_n \cup \{y \oplus 1 | y \in Y_n\}$ , вместо некоторых значений из  $C$  подставлены значения из  $\{0, 1\}$  и при этом хотя бы в одном блоке осталось хотя бы 2 переменные  $\notin Y_n \cup C$  или хотя бы одна переменная  $\in C$ , на более чем  $\frac{7}{8}$  входов, в которой каждый гейт нетривиально зависит от обоих своих входов, можно либо подставить вместо одной из переменных не из  $Y_n \cup C$ , значение из  $\{0, 1\} \cup Y_n \cup \{y \oplus 1 | y \in Y_n\}$  так, чтобы при этом исключилось как минимум 2 гейта, либо подставить вместо  $z \in Y_n$  значение из  $Y_n \setminus z \cup \{y \oplus 1 | y \in Y_n \setminus z\}$ , либо подставить вместо  $c \in C$  значение из  $\{0, 1\}$  так, чтобы при этом исключить как минимум 1 гейт. Все это можно сделать так, чтобы полученная схема совпала с  $G$  на более чем  $\frac{7}{8}$  оставшихся входов.

**Доказательство.** Пусть  $g$  – гейт, входы в который ведут из вершин схемы. По лемме 4 такой гейт существует. Заметим, что все случаи, которые рассматривались в утверждениях 1 и 2, остаются верными. Осталось рассмотреть случай, когда одним из входов  $g$  является  $c \in C$ . Тогда подставим вместо  $c$  значение из  $\{0, 1\}$  так, чтобы полученная в результате схема по-прежнему вычисляла  $G$  на более чем  $\frac{7}{8}$  оставшихся входов.

□

На каждом шаге мы либо подставляем “хорошую” переменную, либо подставляем переменную из  $Y_n$ , либо подставляем переменную из  $C$ . При этом, пока существует блок, в котором есть хотя бы 2 переменные не из  $Y_n \cup C$  или хотя бы одна переменная из  $C$ , полученные описанным в утверждениях 1–3 способом схемы удовлетворяют условию утверждения 3. Таким образом, в каждом блоке из  $2n$  переменных получается по  $n - 2$  “хорошие” переменные и по  $n$  переменных, подстановка значений которым устраняет 1 гейт, а в каждом блоке из  $\alpha n$  переменных – по  $\alpha n - 2$  “хорошие”. Итого,  $m_1(2(n - 2) + n) + m_2(2(\alpha n - 2)) = m_1(3n - 4) + m_2(2\alpha n - 4)$ .

□

**Утверждение 4.** Следующие нижние и верхние оценки верны:

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

**Доказательство.** Все верхние оценки очевидно следуют из того, что  $f_n$  можно вычислить за  $n + 1$  гейт,  $f_n^{-1}$  – за  $2n - 2$  (см. теорему 2), а “ $\oplus_{c_1}$ ” – за  $n$  гейтов. Нижняя оценка следует из теоремы 5.

□

Чтобы порядок надежности построенного семейства был оптимален, нам необходимо подобрать значение  $\alpha$ , максимизирующее

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

$$\min \left\{ \frac{3 + 2\alpha}{3 + \alpha}, \frac{3 + 2\alpha}{1 + 2\alpha} \right\}.$$

Нетрудно видеть, что правая дробь убывает, а левая возрастает. Поэтому максимум достигается при равенстве. А равенство достигается при  $\alpha = 2$ . Следовательно, оптимальное значение порядка надежности —  $\frac{7}{5}$ .

**Замечание 4.** *Руководствуясь теоремами 4 и 5, можно построить на базе приведенного семейства семейство функций с секретом со сверхполиномиальными гарантиями надежности.*

## 6 Заключение

В настоящей работе были разработаны первые конструкции *нелинейных* слабо надежных криптографических примитивов. При этом был совсем незначительно улучшен порядок надежности для надежных в слабом смысле функций с секретом (с  $\frac{25}{22}$  до  $\frac{7}{5}$ ), а также достигнут максимальный на данный момент порядок надежности для функций, односторонних в слабом смысле (2), причем доказательство, представленное в настоящей работе, значительно проще, чем в [Hil92].

Естественные направления дальнейших исследований — улучшение порядков надежности (хотя бы незначительное, ибо для того, чтобы сложность взломщика более чем в 4 раза превосходила сложность честных участников протокола, необходимо улучшить максимальную нижнюю оценку на схемную сложность функции из  $B_{n,n}$ , неизменную уже более 20 лет, а чтобы доказать более чем линейные оценки, скорее всего, придется изобрести что-нибудь посильнее, чем исключение гейтов) для уже существующих видов слабо надежных криптографических примитивов и конструирование новых.

## 7 Благодарности

Автор благодарит своего научного руководителя Эдуарда Алексеевича Гирша за идею данной работы и Григория Ярославцева за ценное дополнение.

## Список литературы

- [Hil92] Alain P. Hiltgen. Constructions of feebly one-way families of permutations. In Proc. of AsiaCrypt '92, pages 422-434, 1992.
- [HN09] Edward A. Hirsch, Sergey I. Nikolenko. A feebly trapdoor function. Proceedings of CSR-2009, LNCS 5675, Springer, pp. 129-142.
- [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 Transparencies and Transparencies from EUROCRYPT '96 IACR. Lecture.
- [Weg87] Ingo Wegener. The Complexity of Boolean Functions. B. G. Teubner, and John Wiley & Sons, 1987.