ВЫЧИСЛИТЕЛЬНО АСИММЕТРИЧНЫЕ ПРЕОБРАЗОВАНИЯ И СХЕМЫ ИЗ ОБРАТИМЫХ ЭЛЕМЕНТОВ

***Жуков Алексей Евгеньевич**, кандидат физико-математических наук, доцент, г. Москва*
***Закаблуков Дмитрий Владимирович**, г. Москва*
***Засорина Юлия Владимировна**, г. Москва*
***Чикин Антон Александрович**, г. Москва*

Понятие однонаправленной функции является одним из важнейших для современной криптографии. Однако строгих доказательств существования или возможности построения таких функций в настоящее время нет. В данной работе будет рассмотрен один подход, позволяющий новым образом взглянуть на явление однонаправленности. Суть подхода заключается в применении обратимых схем для реализации вычислительно асимметричных преобразований. Рассматриваются обратимые схемы, реализующие линейные и нелинейные асимметричные преобразования, двоичное сложение/вычитание, умножение/деление в поле многочленов характеристики 2. Показывается, что разница в сложности прямого и обратного преобразований в некоторых случаях связана с разницей в сложности соответствующих подсхем по уборке вычислительного мусора. На основании рассмотренных обратимых схем делается предположение о структуре вычислительно асимметричных преобразований.

***Ключевые слова**: однонаправленная функция, вычислительно асимметричные преобразования, обратимые схемы, линейные преобразования, нелинейные преобразования, двоичный сумматор, умножение в поле.*

COMPUTATIONALLY ASYMMETRIC TRANSFORMATIONS AND REVERSIBLE LOGIC CIRCUITS

***Alexey Zhukov**, Ph.D., Associate Professor, Moscow*
***Dmitry Zakablukov**, Moscow*
***Yulija Zasorina**, Moscow*
***Anton Chikin**, Moscow*

The concept of one–way function is crucial to the modern cryptography. However, there are no rigorous proofs of the existence or even the possibility of constructing such functions at the moment. In this paper we consider one approach that allows to look in a new way at the phenomenon of one–wayness. The essence of this approach is to use reversible circuits to implement computationally asymmetric transformations. We consider reversible circuits implementing linear and nonlinear asymmetric transformations, binary addition/subtraction, multiplication/division in the field of polynomials of characteristic 2. We show that the difference in the complexity of the direct and inverse transformations in some cases is linked to the difference in the complexity of the sub–circuits, cleaning the computational garbage. Basing on the considered reversible circuits, we make an assumption about the structure of the computationally asymmetric transformations.

***Keywords**: one–way function, computationally asymmetric transformations, reversible logic, linear transformations, nonlinear transformations, binary adder, multiplication in the field.*

Для современной криптографии одним из важнейших понятий является понятие однонаправленной функции. Однако, не смотря на многочисленные работы, посвященные этой тематике, строгих доказательств существования или возможности построения таких функций в настоящее время нет. В данной работе будет рассмотрен один подход, позволяющий новым образом взглянуть на явление однонаправленности.

Говоря неформально, однонаправленная функция – это эффективно вычисляемая функция, для задачи обращения которой не существует эффективных алгоритмов. В качестве модели обратимого преобразования возьмем подстанов-

ку на множестве двоичных наборов; в качестве меры сложности того или иного преобразования – сложность минимальной булевой схемы, реализующей данное преобразование и обозначаемой в дальнейшем через $C(f)$. В качестве модели однонаправленной функции будем рассматривать вычислительно асимметричное преобразование, т.е. такое обратимое преобразование, сложность которого отличается от сложности обратного преобразования.

Широко известным классом вычислительно асимметричных преобразований являются линейные преобразования $\varphi_n : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, изученные в работах [1], [2]:

$$\varphi_n : \begin{cases} y_i(x) = x_i \oplus x_{i+1}, & i < n, \\ y_n(x) = x_1 \oplus x_{\lceil n/2 \rceil} \oplus x_n, & n - \text{нечетно} \end{cases}$$

Соответствующее обратное преобразование имеет вид:

$$\varphi_n^{-1} : \begin{cases} x_i(y) = (y_1 \oplus \ldots \oplus y_{i-1}) \oplus (y_{\lceil n/2 \rceil} \oplus \ldots \oplus y_n), & i \le \lceil n/2 \rceil, \\ x_i(y) = (y_1 \oplus \ldots \oplus y_{\lceil n/2 \rceil - 1}) \oplus (y_i \oplus \ldots \oplus y_n), & i > \lceil n/2 \rceil. \end{cases}$$

В работе [2] доказано, что при n ≥ 5 сложности прямых и обратных преобразований равны соответственно $C(\varphi_n) = n+1$ и $C(\varphi^{-1}{}_n) = \left\lfloor \frac{3}{2}(n-1) \right\rfloor$.

Пытаясь понять природу такого различия, можно задать глупый вопрос: почему схему, реализующую прямое преобразование, нельзя использовать для вычисления обратного преобразования? Ответ очевиден – потому, что логические элементы, отличные от инверсии, необратимы. Однако уже давно известны ***обратимые логические элементы*** [3], примерами которых могут служить такие элементы как NOT, CNOT (Controlled NOT), CCNOT (Controlled Controlled NOT):

Рис. 1. *Элемент NOT*

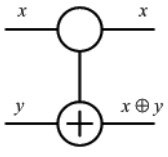

Рис. 2. *Элемент CNOT.*

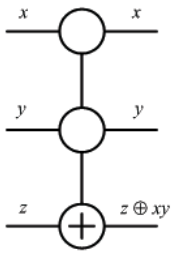

Рис. 3. *Элемент CCNOT.*

С помощью этих элементов можно построить минимальную схему, реализующую данное преобразование. Для удобства изображения схем и получения обратной схемы будем располагать элементы на параллельных горизонтальных линиях, на которые подаются входные переменные. К схеме возможно добавление дополнительных линий, на которые подается логический 0 и играющая роль «памяти».

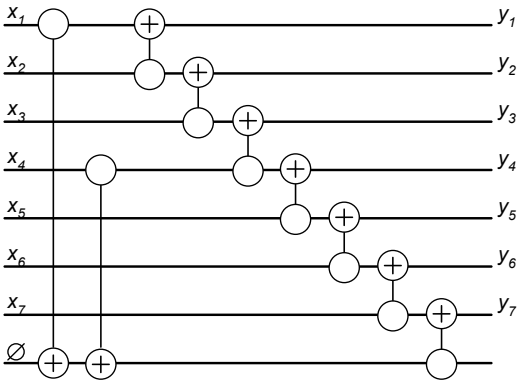

Рис. 4. *Минимальная схема прямого линейного преобразования φ_7.*

Однако и эта схема не будет обратимой. Дело в том, что в процессе вычисления нашего преобразования на выходе схемы появился не только вектор $(y_1,\ldots,y_7)$, но некоторая информация (на выходе дополнительной линии), полученная в процессе вычисления и называемая ***вычислительным мусором*** или просто ***мусором***. Без знания этой информации, а только по $(y_1,\ldots,y_7)$ вход $(x_1,\ldots,x_7)$ получить невозможно. В то же время схема, изображенная на рис. 5, будет реализовывать как прямое, так и обратное преобразования в зависимости от того, с какой стороны подавать информацию.

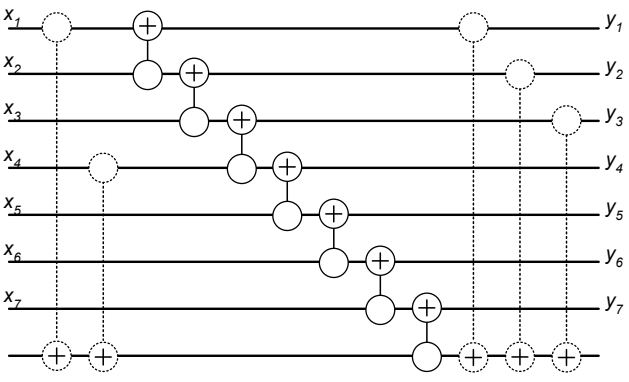

Рис. 5. *Схема обратимого линейного преобразования φ_7.*

Обратимая схема будет содержать некоторые «лишние» элементы (отмеченные пунктиром), которые не нужны для реализации, например, прямого преобразования, но нужны для реализа-

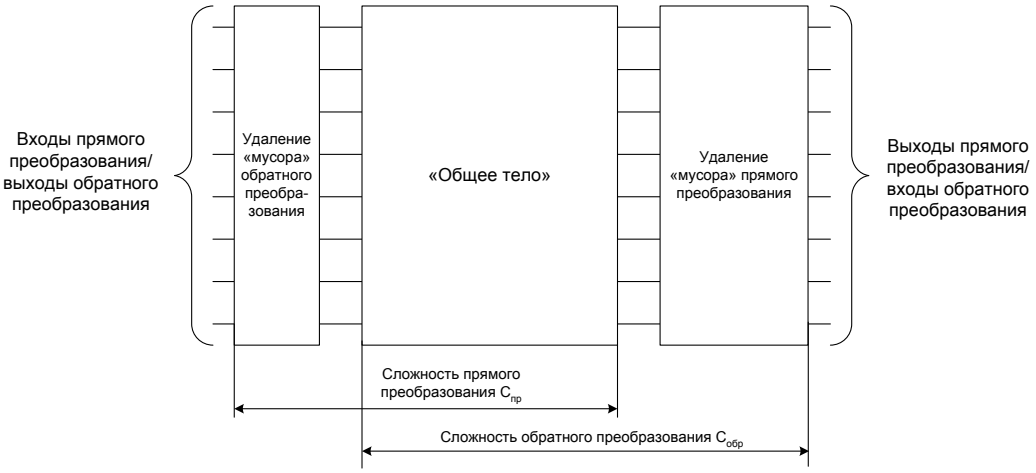

Рис. 6. *Возможная структура асимметричных преобразований.*

ции обратного преобразования, и наоборот. Рассмотрим, какую роль выполняют эти элементы. Исходная схема (рис. 4) необратима, так как для корректного вычисления в обратную сторону нам необходимо подать на дополнительную линию соответствующий «мусор», который в общем случае неизвестен. Для того чтобы схема стала обратимой, надо обнулить «мусор», что достигается введением в схему дополнительных элементов, отмеченных пунктиром в правой части рис. 5. В обратной же схеме эти элементы будут выполнять необходимые для обратного преобразования функции.

Проанализировав построенную схему из обратимых элементов, можно выдвинуть следующую гипотезу о структуре вычислительно асимметричных преобразований. В ходе работы прямой схемы вычислительно асимметричного преобразования, получается некоторая дополнительная информация («мусор», с криптографической точки зрения играющий роль «лазейки»), которая необходима для получения результата прямого преобразования. При попытке непосредственного обращения по такой схеме, на ее входы необходимо будет подать этот «мусор», который в общем случае неизвестен. Поэтому, чтобы получить обратимую схему, необходимо добавить в нее дополнительные элементы, которые будут удалять «мусор». Возможно, что схемы из обратимых элементов для асимметричных преобразований имеют следующую общую структуру, которая показана на рис. 6. У таких схем есть некоторое «общее тело», а также подсхемы, отвечающие за удаление «мусора» прямого и обратного преобразований. Из-за разницы в сложностях этих подсхем удаления «мусора» и возникает разница в сложности прямого и обратного преобразований.

Аргументами в пользу сформулированной выше гипотезы служат обратимые схемы, построенные для таких известных вычислительно асимметричных преобразований, как нелинейные асимметричные преобразования [2] и двоичный сумматор/вычитатель [4]. Эти схемы, а также умножитель в поле многочленов характеристики 2 будут рассмотрены далее.

Схема асимметричного нелинейного преобразования

В работе А. Хилтгена [2] представлено нелинейное асимметричное преобразование. Оно представляет собой композицию двух преобразований, одно из которых (α_n) линейно, а второе (β_n) — нелинейно и, к тому же, является инволюцией, то есть обратное преобразование совпадает с прямым.

Преобразования задаются следующими формулами:

$$\alpha_n : \begin{cases} z_i(x) = x_i \oplus x_{i+1} & i < n, \\ z_i(x) = x_i & i = n. \end{cases}$$

$$\beta_n : \begin{cases} y_i(z) = z_i \\ y_i(z) = z_n \oplus \left[\overline{(z_1 \oplus \ldots \oplus z_{n-2})} \wedge z_{n-1} \right] \end{cases} \quad \begin{matrix} i < n, \\ i = n. \end{matrix}$$

Соответствующие обратные преобразования задаются формулами:

$$\beta_n^{-1} : \begin{cases} z_i(y) = y_i \\ z_i(y) = y_n \oplus \left[\overline{(y_1 \oplus \ldots \oplus y_{n-2})} \wedge y_{n-1} \right] \end{cases} \quad \begin{matrix} i < n, \\ i = n. \end{matrix}$$

$$\alpha_n^{-1} : \begin{cases} x_i(z) = z_i \oplus \ldots \oplus z_n & i < n, \\ x_i(z) = z_n & i = n. \end{cases}$$

Композиция этих преобразований дает преобразование следующего вида:

$$\gamma_n(x) = \beta_n(\alpha_n(x)): \begin{cases} y_i(x) = x_i \oplus x_{i+1} & i < n, \\ y_i(x) = x_n \oplus \left[\overline{(x_1 \oplus x_{n-1})} \wedge (x_{n-1} \oplus x_n) \right] & i = n. \end{cases}$$

$$\gamma_n^{-1}(y) = \alpha_n^{-1}(\beta_n^{-1}(x)): \begin{cases} x_i(y) = (y_1 \oplus \ldots \oplus y_n) \oplus \left[\overline{(y_1 \oplus \ldots \oplus y_{n-2})} \wedge y_{n-1} \right] & i < n, \\ x_i(y) = y_n \oplus \left[\overline{(y_1 \oplus \ldots \oplus y_{n-2})} \wedge y_{n-1} \right] & i = n. \end{cases}$$

Доказано, что при $n \geq 4$ комбинационная сложность прямого и обратного преобразований составляют соответственно:

$$C(\gamma_n) = n + 2 \qquad C(\gamma_n^{-1}) = 2(n-1)$$

Обратимые схемы, реализующие прямое и обратное преобразование для различных значений n, были получены Засориной Ю.В.[1]

Рассмотрим схему прямого преобразования для случая $n = 6$.

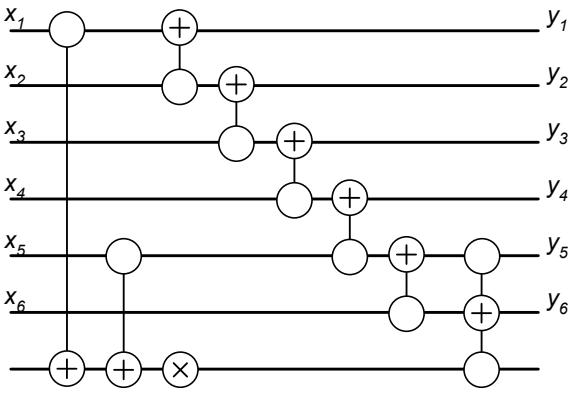

***Рис. 7**. Схема прямого нелинейного преобразования.*

Как и в случае схемы линейного преобразования, для получения обратимой схемы нам также потребуется удаление «мусора», образовавшегося на нижней, дополнительной линии. «Мусор» в данном случае равен $x_1 \oplus x_5$, и его можно удалить, инвертировав значение на этой линии и прибавив значения, снятые с первой, второй, третьей и четвертой линий. Получаем схему, показанную на рис. 8.

Рассматривая эту схему справа налево, можно заметить, что она полностью, кроме элементов, нарисованных пунктиром, соответствует выражению, описывающему обратное преобразование. Элементы, нарисованные пунктиром, удаляют «мусор», возникающий при обратном преобразовании, а элементы, обведенные пунктирным прямоугольником, удаляют «мусор» прямого преобразования.

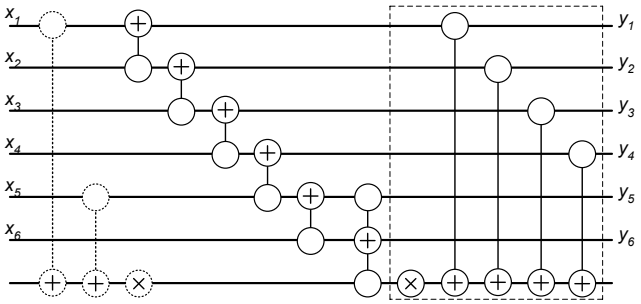

***Рис. 8**. Обратимая схема нелинейного преобразования.*

Двоичный сумматор

Рассмотрим операцию сложения двух n-разрядных чисел A и B. Данную операцию можно описать булевым отображением $f(\mathbf{a}, \mathbf{b}) = \mathbf{s}$, где $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n$, $\mathbf{s} \in \mathbb{Z}_2^{n+1}$ – двоичные вектора слагаемых A и B и суммы $S = A + B$ соответственно.

Можно построить схему над базисом двуместных булевых функций, реализующую отображение $f(\mathbf{a}, \mathbf{b})$. Обозначим через $L(n)$ сложность этой схемы, а через $D(n)$ – ее глубину. В работе [4] Редькиным Н.П. было доказано, что $L(n) = 5n - 3$. При этом глубина такой схемы удовлетворяет неравенству $D(n) \leq 2n - 1$ [5].

Отображение $f(\mathbf{a}, \mathbf{b})$ также может быть реализовано обратимой схемой, состоящей из вентилей NOT, CNOT и 2-CNOT. Чикиным А.А. была предложена[2] такая обратимая схема (рис. 9).

1 Результаты получены Засориной Ю.В. в 2007 г. в рамках авторского дипломного проектирования по теме «Вычислительно асимметричные преобразования и схемы из обратимых элементов» согласно учебным планам кафедры ИУ8.

2 Результаты получены Чикиным А.А. в 2005 г. в рамках авторской курсовой работы по теме «Двоичный обратимый сумматор из обратимых элементов» согласно учебным планам кафедры ИУ8.

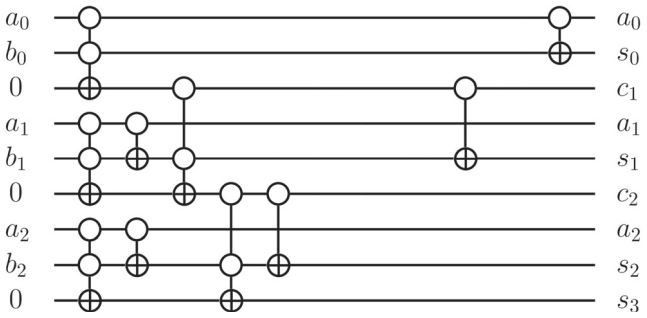

***Рис. 9**. Обратимая схема двоичного сумматора без уборки мусора.*

Было показано, что эта обратимая схема имеет вентильную сложность $L(n)=4n-2$ и глубину $D(n)\le n+2$. Снижение этих величин по сравнению с оценками, данными в работах [4,5] связано с особенностью обратимых схем и с использованием вентилей 2-CNOT, которые реализуют одновременно операцию конъюнкции и сложения по модулю 2.

Как видно из рис. 9, данная схема не является полностью обратимой в том смысле, что на выходах схемы получается вычислительный мусор: значение переносов c_i. Чикиным А.А. также была предложена обратимая схема, реализующая двоичный сумматор с уборкой мусора (рис. 10). Данная схема имеет следующие характеристики: $L(n)=7(n-1)$, $D(n)\le 5n-4$. Увеличение вентильной сложности и глубины данной схемы связано с уборкой мусора на выходах.

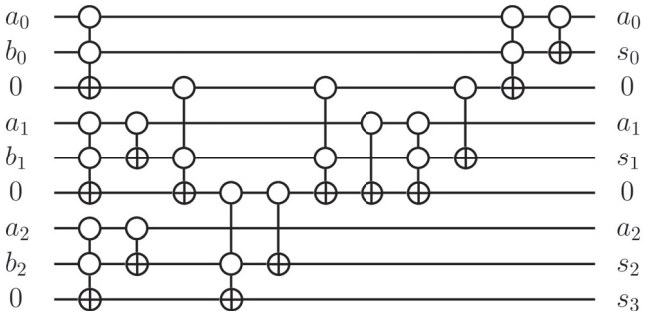

***Рис. 10.** Обратимая схема двоичного сумматора с уборкой мусора.*

Из обратимой схемы, не содержащей вычислительного мусора на своих выходах, легко получить обратимую схему, реализующую отображение, обратное к заданному. Таким способом Чикиным А.А. была получена схема двоичного вычитателя (рис. 11).

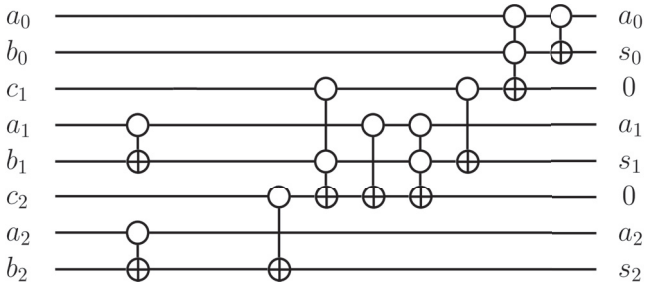

***Рис. 11**. Обратимая схема двоичного вычитателя без уборки мусора.*

Для более ясного понимания связи этой схемы с предыдущей, на рис. 11 входы схемы расположены справа, а выходы – слева. Обратимая схема двоичного вычитателя имеет следующие характеристики: $L(n)=5n-6$, $D(n)\le 4(n-1)$. Стоит отметить, что эти характеристики асимптотически выше по сравнению с характеристиками обратимой схемы двоичного сумматора. Это объясняется разницей в подсхемах по уборке вычислительного мусора в том и другом случае.

Умножение в поле многочленов

Рассмотрим операцию умножения двух многочленов A и B в поле $\mathsf{F}_2[x]/f(x)$, где $f(x)$ – неприводимый многочлен степени n. Данную операцию можно описать булевым преобразованием $f_{\text{mul}}(\mathbf{a},\mathbf{b})=(\mathbf{a},\mathbf{c})$, где $\mathbf{a},\mathbf{b},\mathbf{c}\in\mathbb{Z}_2^n$ – двоичные вектора коэффициентов многочленов $A,B,C\in\mathsf{F}_2^*[x]/f(x)$, $C=A*B$. Обратное преобразование $f_{\text{mul}}^{-1}(\mathbf{a},\mathbf{c})$ описывает операцию деления многочлена C на многочлен A в этом поле.

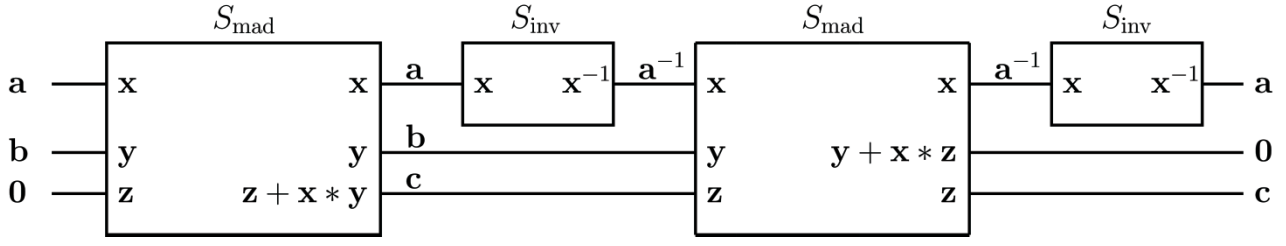

***Рис. 12**. Обратимая схема умножения многочленов в поле $\mathsf{F}_2[x]/f(x)$.*

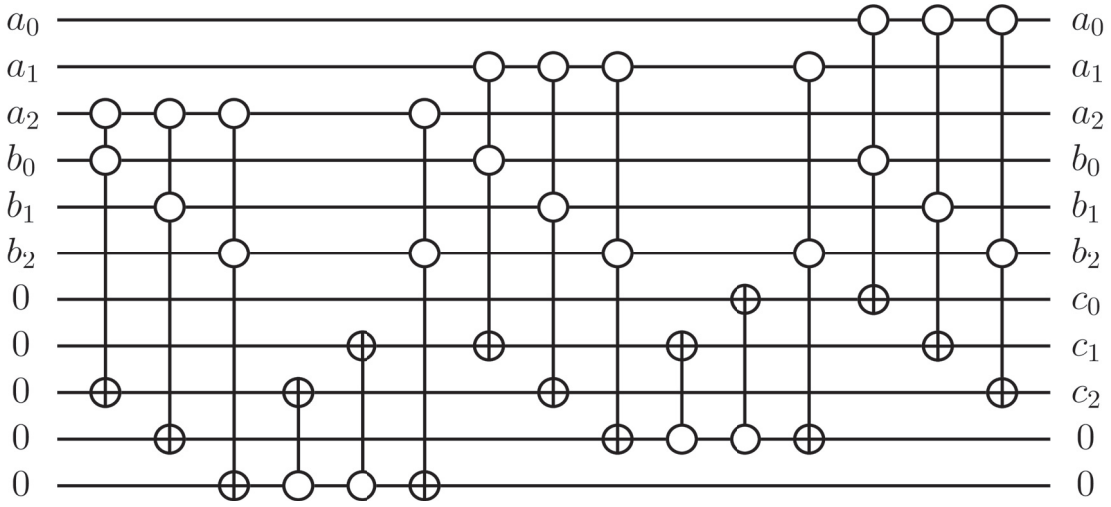

Рис. 13. *Обратимая схема умножения многочленов в поле* $\mathsf{F}_2[x]/(x^3+x+1)$ *с частичной уборкой вычислительного мусора (* S_{mad} *).*

Закаблуковым Д.В. было показано[3], что преобразование $f_{\text{mul}}(\mathbf{a},\mathbf{b})$ может быть реализовано обратимой схемой, структура которой показана на рис. 12.

По данному рисунку видно, что обратимая схема умножения S_{mul} с порождением вычислительного мусора будет равна подсхеме S_{mad} – схеме умножения со сложением. Деление многочленов в поле можно выразить через умножение на многочлен, обратный к многочлену делителя. В схеме на рис. 12 это обращение многочлена реализуется схемой S_{inv}. Таким образом, обратимая схема деления S_{div} с порождением вычислительного мусора будет равна композиции подсхем S_{inv} и S_{mad}. Отсюда следуют следующие неравенства для вентильной сложности и глубины схем S_{mul} и S_{div}:

$$L(S_{\text{mul}}) \le L(S_{\text{mad}}),\ D(S_{\text{mul}}) \le D(S_{\text{mad}}),$$
$$L(S_{\text{div}}) \le L(S_{\text{inv}}) + L(S_{\text{mad}}),$$
$$D(S_{\text{div}}) \le D(S_{\text{inv}}) + D(S_{\text{mad}})$$

Закаблуковым Д.В. был использован самый простой алгоритм умножения «столбиком». На рис. 13 представлена полученная им обратимая схема S_{mul} для поля $\mathsf{F}_2[x]/(x^3+x+1)$. В общем случае такая схема имеет следующие характеристики:

$$L(S_{\text{mul}}) = D(S_{\text{mul}}) = n^2 + (n-1)\cdot w(f(x)) \le 2n^2 + 1$$

где $w(f(x))$ – количество единичных коэффициентов многочлена $f(x)$. Можно уменьшить эти характеристики на $n-1$, если не убирать вычислительный мусор с $(n-1)$ нижних выходов: $L(S_{\text{mul}}) = D(S_{\text{mul}}) \le 2n^2 - n$.

Закаблуковым Д.В. также были рассмотрены различные способы обращения многочлена в поле $\mathsf{F}_2[x]/f(x)$. В том числе была изучена возможность применения расширенного алгоритма Евклида для этой цели. Однако основная сложность при реализации данного алгоритма в обратимой схеме заключается в том, что необходимо на каждом этапе работы сначала вычислить степень многочлена-делителя, а затем для всех возможных значений этой степени реализовать алгоритм деления многочлена с остатком. Дальнейшее описание способа построения обратимой схемы, реализующей расширенный алгоритм Евклида, и характеристики схем взяты из авторского дипломного проекта.

Обратимая схема, реализующая расширенный алгоритм Евклида, состоит из n подсхем $S^{n,k}_{\text{euclid}}$ – по количеству шагов данного алгоритма. Каждая такая подсхема принимает на вход вектора коэффициентов делимого многочлена, многочлена-делителя и многочлена-результата. При этом старшие коэффициенты в этих векторах не обязательно равняются 1 – для делимого многочлена это означает, что на данном шаге не надо делить, а просто уменьшить размерность векторов и перейти к следующему шагу алгоритма.

Вначале строится подсхема S^n_{deg}, определяющая степень многочлена-делителя: $L(S^n_{\text{deg}}) = D(S^n_{\text{deg}}) = 3n-2$. Если старший коэф-

3 Результаты получены Закаблуковым Д.В. в 2012 г. в рамках авторского дипломного проектирования по теме «Исследование эффекта однонаправленности преобразований на основе схем из обратимых логических элементов» согласно учебным планам кафедры ИУ8.

фициент делимого многочлена равен 0, то происходит копирование входов на выходы с уменьшением размерности векторов. Если же он равен 1, то происходит копирование входов на входы параллельных подсхем $S^{n,m,k}_{\text{step}}$, реализующих деление для всех возможных степеней многочлена делителя. Для делимого многочлена степени n таких подсхем будет n. Данное копирование производится при помощи подсхемы $S^{n,k}_{\text{copy}}$, ее характеристики:

$$L(S^{n,k}_{\text{copy}}) = (n+k)(n-1) + \sum_{i=1}^{n-1} i + 3n + k - 3$$

$$D(S^{n,k}_{\text{copy}}) = \max(\lceil \log_2 n \rceil, \lceil \log_2 k \rceil) + 3n + k - 3$$

Для каждой из параллельных подсхем $S^{n,m,k}_{\text{step}}$ требуется: $(n-m+1)(m+1)$ вентилей для вычисления частного и остатка, $(n-m+1)k$ вентилей для умножения частного на многочлен-результат, m вентилей для копирования делителя (новое значение n), $(m-1)$ вентилей для копирования остатка (новое значение m), $(n-m+k)$ вентилей для копирования результата умножения (новое значение k). В итоге получаем следующие характеристики:

$$L(S^{n,m,k}_{\text{step}}) = D(S^{n,m,k}_{\text{step}}) = (n-m+1)(m+k+1) + n + m + k - 1$$

Для характеристик схемы $S^{n,k}_{\text{euclid}}$, реализующей один шаг расширенного алгоритма Евклида, верны следующие равенства:

$$L(S^{n,k}_{\text{euclid}}) = L(S^{n-1}_{\text{deg}}) + L(S^{n,k}_{\text{copy}}) + \sum_{i=1}^{n-1} L(S^{n,i,k}_{\text{step}})$$

$$D(S^{n,k}_{\text{euclid}}) = D(S^{n-1}_{\text{deg}}) + D(S^{n,k}_{\text{copy}}) + \max_{i=1}^{n-1} D(S^{n,i,k}_{\text{step}})$$

Тогда для характеристик схемы S_{inv} верны следующие равенства (оценки получены при помощи ПО Maple):

$$L(S_{\text{inv}}) = \sum_{i=2}^{n+1} L(S^{i,n-i+2}_{\text{euclid}}) = \frac{n^4}{12} + \frac{7n^3}{3} + \frac{119n^2}{2} + \frac{17n}{3} = O(n^4)$$

$$D(S_{\text{inv}}) = \sum_{i=2}^{n+1} D(S^{i,n-i+2}_{\text{euclid}}) = \frac{n^3}{4} + \frac{13n^2}{2} + \frac{29n}{4} + O(n\log_2 n) = O(n^3)$$

Таким образом, для характеристик схемы S_{div} верны следующие неравенства:

$$L(S_{\text{div}}) = O(n^4),\ D(S_{\text{div}}) = O(n^3)$$

Из этих соотношений видно, что деление двух многочленов A и B в поле $\mathsf{F}_2[x]/f(x)$, где $f(x)$ – неприводимый многочлен степени n, можно реализовать обратимой схемой с полиномиальной вентильной сложностью и глубиной. Однако даже глубина такой схемы будет на порядок выше глубины обратимой схемы, реализующей умножение многочленов в этом же поле.

Литература

1. Boppana R.B., Lagarias J.C. One-way functions and circuit complexity // Information and Computation. 1987. Vol. 74(3). P. 226-240. doi:10.1016/0890-5401(87)90022-8
2. Hiltgen A.P. Cryptographically Relevant Contributions to Combinatorial Complexity Theory // ETH Series in Information Processing. 1994. Vol. 3.
3. Toffoli M. Bicontinuous Extensions of Invertible Combinatorial Functions // Math. Syst. Theory. 1981. Vol. 14. P. 13-23.
4. Редькин Н.П. О минимальной реализации двоичного сумматора // Проблемы кибернетики. М: Матгиз, 1981. Вып. 38. С. 181-216.
5. Гашков С.Б., Гринчук М.И., Сергеев И.С. О построении схем сумматоров малой глубины // Дискретный анализ и исследование операций. Серия 1. – 2007. – Т. 14, № 1. – С. 27-44. doi:10.1134/S1990478908020038

Reference

1. Boppana R.B., Lagarias J.C. One-way functions and circuit complexity // Information and Computation. 1987. Vol. 74(3). P. 226-240. doi:10.1016/0890-5401(87)90022-8
2. Hiltgen A.P. Cryptographically Relevant Contributions to Combinatorial Complexity Theory // ETH Series in Information Processing. 1994. Vol. 3.
3. Toffoli M. Bicontinuous Extensions of Invertible Combinatorial Functions // Math. Syst. Theory. 1981. Vol. 14. P. 13-23.
4. Red'kin N.P. O minimal'noy realizatsii dvoichnogo summatora, Problemy kibernetiki. M: Matgiz, 1981, Vyp. 38, pp. 181-216.
5. Gashkov S.B., Grinchuk M.I., Sergeev I.S. O postroenii skhem summatorov maloy glubiny, Diskretnyy analiz i issledovanie operatsiy, Seriya 1, 2007, V. 14, N 1, pp. 27-44. doi:10.1134/S1990478908020038