ПЕРЕМЕШИВАЮЩИЕ СВОЙСТВА ОПЕРАЦИЙ, ОПРЕДЕЛЕННЫХ НА МНОЖЕСТВЕ *N*-МЕРНЫХ ВЕКТОРОВ НАД ПРОСТЫМ КОНЕЧНЫМ ПОЛЕМ

Л. В. Ковальчук, Н. В. Лысенко, Л. В. Скрыпник

Институт специальной связи и защиты информации НТУУ «КПИ»
Киев, Украина
E-mail: lv_kov_crypto@mail.ru, ndemy@mail.ru

В работе получены результаты, характеризующие влияние операции поразрядного/модульного сложения на множестве векторов над простым конечным полем на структуру фактор-группы по определенной подгруппе относительно операции модульного/поразрядного сложения на этом же множестве. Показано, что перемешивающие свойства операций модульного сложения зависят от выбора подгруппы относительно операции поразрядного сложения.

Ключевые слова: кольцо вычетов, факторгруппа, перемешивающие свойства операций, операции поразрядного и модульного сложения.

Введение

Одной из задач современной прикладной криптографии является создание криптографических примитивов, которые стойки к различным современным атакам, просты и удобны в реализации. Поэтому возникает вопрос о нахождении такого набора операций на множестве *p*-арных (*p* – простое число) векторов (открытых текстов), которые реализуются и программным, и аппаратным способом, а с другой – обладают «хорошими перемешивающими свойствами». Чередование операций, обладающих такими свойствами, обеспечивает стойкость примитива к различным алгебраическим и статистическим атакам, что позволяет строить примитивы с простой и удобной в реализации структурой.

В работе М. Шемякиной [1] получены результаты, характеризующие перемешивающие свойства операций в конечном поле (которые оказались очень хорошими) и перемешивающие свойства операции модульного сложения и унарной операции взятия обратного элемента (оказались плохими).

Далее, в работах Л. Ковальчук и О. Сиренко [2, 3] получены результаты, которые характеризуют перемешивающие свойства операций побитового и модульного сложения, заданных на одном носителе.

В работе Б. Погорелова, М. Пудовкиной [4] получены результаты относительно наличия нетривиальных факторструктур для преобразований аддитивных групп, в частности, обобщен тот результат Л. Ковальчук и О. Сиренко, который касается существования инвариантных подгрупп в аддитивной группе кольца Z_{2^n} и в линейном пространстве V_n. Однако в работе [4] доказывается только существование инвариантных подгрупп, но не вычисляются вероятности попадания в различные классы смежности при сложении элементов, принадлежащих классам смежности по неинвариантной подгруппе.

В статье обобщены результаты Л. Ковальчук и О. Сиренко для операций поразрядного и модульного сложения. Показано, что в зависимости от выбора подгруппы

в $V_n(p)$ операция модульного сложения в Z_{p^n} может как существенно разрушать структуру факторгруппы по выбранной подгруппе, так и полностью ее сохранять. Также показано, что для любой подгруппы в Z_{p^n} операция поразрядного сложения всегда сохраняет структуру соответствующей факторгруппы.

Вспомогательные обозначения и результаты

При доказательстве основных результатов будут использованы следующие обозначения и утверждения. Здесь и далее под $(V_n(p),\oplus_p)$ будем понимать множество векторов длины n с операцией поразрядного сложения по модулю простого числа p, а под $(Z_{p^n},+)$ – аддитивную группу кольца вычетов с операцией сложения по модулю p^n. Каждому целому числу $z \in Z_{p^n}$ поставим в соответствие вектор длины n, p-арное представление этого числа. Таким образом мы отождествили множества Z_{p^n} и $V_n(p)$. Целое число и соответствующий ему p-арный вектор будем обозначать одинаково; из контекста следует, какое представление используется.

Для любого $t \geq 0$ введем следующие обозначения:

$$s_t = \left(\frac{1}{2} + \frac{1}{2p^t}\right); \quad q_t = 1 - s_t.$$

Обозначение вида

$$\underbrace{\ldots}_{b_{k+1}\text{разрядов}}\underbrace{0\ \ldots\ 0}_{a_k\text{разрядов}}\underbrace{\ldots}_{b_k\text{разрядов}}\ldots\underbrace{0\ \ldots\ 0}_{a_1\text{разрядов}}\underbrace{\ldots}_{b_1\text{разрядов}}$$

будем использовать для p-арного вектора длины $n = \sum_{i=1}^{k} a_i + \sum_{i=1}^{k+1} b_i$, у которого слева b_{k+1} произвольных разрядов, далее a_k нулевых разрядов, и т. д.

Влияние операции модульного сложения на структуру факторгруппы $(V_n(p),\oplus_p)$ по ее подгруппе

Определение 1. Обозначим через $G(a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k, b_{k+1})$ подгруппу индекса p^a группы $(V_n(p),\oplus_p)$, элементы которой содержат k «нулевых» блоков $A_1, A_2, \ldots, A_k$, сумма длин которых равна a, т. е. имеют следующую структуру:

$$\underbrace{\text{блок } B_{k+1}}_{b_{k+1}\text{ разрядов}}\ \underbrace{\text{блок } A_k}_{a_k\text{ разрядов}}\ \underbrace{\text{блок } B_k}_{b_k\text{ разрядов}}\ \ldots\ \underbrace{\text{блок } A_2}_{a_2\text{ разрядов}}\ \underbrace{\text{блок } B_2}_{b_2\text{ разрядов}}\ \underbrace{\text{блок } A_1}_{a_1\text{ разрядов}}\ \underbrace{\text{блок } B_1}_{b_1\text{ разрядов}},$$

$$\underbrace{\ldots}\ \underbrace{0\ \ldots\ 0}\ \underbrace{\ldots}\ \ldots\ \underbrace{0\ \ldots\ 0}\ \underbrace{\ldots}\ \underbrace{0\ \ldots\ 0}\ \underbrace{\ldots}$$

где разряды из «ненулевых» блоков $B_1, ..., B_{k+1}$ принимают произвольные значения, причем $\sum_{i=1}^{k} a_i = a, \sum_{i=1}^{k} b_i = b,$ и $a + b + b_{k+1} = n; a_i > 0, b_i > 0$ при $i = 2, ..., k;$ $b_1 \geq 0,$ $b_{k+1} \geq 0$.

Тогда в наших обозначениях справедлива следующая теорема.

Теорема 1. Пусть $G(a_1, a_2, ..., a_k, b_1, b_2, ..., b_k, b_{k+1})$ – некоторая подгруппа индекса p^a группы $(V_n(p), \oplus_p)$; c и d – случайные элементы, которые равновероятно распределены в классах смежности H_i и H_j подгруппы G соответственно; $i, j = 1, ..., p^a$. Тогда:

1) количество классов смежности по подгруппе G, в которые сумма элементов c и d по модулю p^n попадает с ненулевой вероятностью, равно

$$2^k, \text{ если } b_1 > 0, \text{ и } 2^{k-1}, \text{ если } b_1 = 0,$$

а количество классов смежности, в которые сумма элементов c и d по модулю p^n попадает с нулевой вероятностью, равно

$$p^a - 2^k, \text{ если } b_1 > 0, \text{ и } p^a - 2^{k-1}, \text{ если } b_1 = 0;$$

2) если $H_i = H_j$, то классы смежности, в которые разность элементов c и d по модулю p^n попадает с ненулевой вероятностью, имеют следующий вид:

$$\underbrace{\text{блок } B_{k+1} \ \ldots}_{b_{k+1} \text{ разрядов}} \underbrace{\text{блок } A_k \ \ldots}_{a_k \text{ разрядов}} \underbrace{\text{блок } B_k \ \ldots}_{b_k \text{ разрядов}} \ldots \underbrace{\text{блок } A_1 \ \ldots}_{a_1 \text{ разрядов}} \underbrace{\text{блок } B_1 \ \ldots}_{b_1 \text{ разрядов}},$$

где блоки A_l содержат либо только 0, либо $p-1$, для любого $l = 1, ..., k$, и количество этих классов смежности равно

$$2^k, \text{ если } b_1 > 0, \text{ и } 2^{k-1}, \text{ если } b_1 = 0;$$

а количество классов смежности по подгруппе G, в которые разность элементов c и d по модулю p^n попадает с ненулевой вероятностью, равно

$$p^a - 2^k, \text{ если } b_1 > 0, \text{ и } p^a - 2^{k-1}, \text{ если } b_1 = 0.$$

При этом вероятности попадания разности элементов c и d в различные классы смежности одинаковы при любом выборе класса смежности H_i (т. е. класса смежности, которому принадлежат c и d), и будут зависеть только от вида подгруппы, по которой строятся эти классы смежности.

3) ненулевые вероятности попадания суммы (разности) элементов c и d по модулю p^n в соответствующие классы смежности будут лежать в пределах от $\prod_{i=1}^{k} q_{b_i}$ до $\prod_{i=1}^{k} s_{b_i}$.

Следует отметить, что если в подгруппе имеются только «нулевые» блоки единичной длины, то количество классов смежности, в которые сумма векторов по

модулю p^n будет попадать с ненулевой вероятностью, будет наибольшим; если «нулевые» блоки будут большой длины, то количество классов смежности, в которые сумма векторов по модулю p^n будет попадать с ненулевой вероятностью, уменьшается. Чем длиннее «нулевые» блоки, тем в меньшее количество классов смежности попадает сумма векторов по модулю p^n с ненулевой вероятностью. Таким образом, перемешивающие свойства операции модульного сложения относительно поразрядного сложения зависят от структуры подгруппы.

Влияние операции поразрядного сложения на структуру факторгруппы $\left(Z_{p^n},+\right)$ по ее подгруппе индекса p^k относительно модульного сложения

Теорема 2. Пусть G_k подгруппа $\left(Z_{p^n},+\right)$ индекса p^k. Тогда:

a) G_k (в соответствующем представлении) – подгруппа $\left(V_n(p),\oplus_p\right)$;

b) классы смежности по подгруппе G_k (относительно операции +) имеют вид $i+G_k, 0\le i<p^k$, а классы смежности по подгруппе G_k (относительно операции $\oplus_p$) имеют вид $i\oplus_p G_k$, причем $i\oplus_p G_k = i+G_k, 0\le i<p^k$;

c) если $c,d\in i\oplus_p G_k$, то с вероятностью 1 выполнено $c-d\in G_k, 0\le i<p^k$;

d) если $c\in i+G_k, d\in j+G_k$, то с вероятностью 1 выполнено $c\oplus_p d\in i\oplus_p j+G_k$, причем класс смежности $i\oplus_p j+G_k$, вообще говоря, не совпадает с $i+j+G_k, 0\le i,j<p^k$;

e) если $c\in i\oplus_p G_k, d\in j\oplus_p G_k$, то с вероятностью 1 выполнено $c+d\in i+j+G_k,\ \ 0\le i,j<p^k$.

Из теоремы можно сделать следующий вывод: если для некоторого $k=0,...,n$ элементы подгруппы имеют вид

$$\underbrace{\ldots}_{n\text{-}k\text{ разрядов}}\ \underbrace{0\ \ldots\ 0}_{k\text{ разрядов}},$$

то операция поразрядного (модульного) сложения сохраняет структуру соответствующей факторгруппы относительно модульного (поразрядного) сложения.

Выводы

Результаты характеризуют перемешивающие свойства операций поразрядного и модульного сложения, заданных на одном носителе. Наиболее интересен тот факт, что действие операции модульного сложения на факторгруппу относительно операции поразрядного сложения существенно зависит от выбора подгруппы в $\left(V_n(p),\oplus_p\right)$,

а операция поразрядного сложения всегда сохраняет структуру соответствующей факторгруппы по любой подгруппе в $\left(Z_{p^n},+\right)$.

Другими словами, полученные результаты свидетельствуют о плохих перемешивающих свойствах рассмотренных операций: во-первых, существует много нетривиальных подгрупп, которые будут подгруппами относительно обеих операций; во-вторых, для таких подгрупп полностью сохраняется структура соответствующей факторгруппы. В терминах атак, базирующихся на гомоморфизмах, можно утверждать, что классы смежности по таким подгруппам создают блоки импримитивности. А наличие таких блоков дает потенциальную возможность реализовать атаки гомоморфизмов. Значит, блоковые шифры, построенные с использованием только операций поразрядного и модульного сложения, уязвимы к таким атакам.

Рассмотренные операции используются в современных алгоритмах шифрования (IDEA – международный алгоритм шифрования данных; ГОСТ 28147-89 – действующий стандарт шифрования в Украине, России и некоторых других странах; «Калина» – претендент на национальный стандарт шифрования Украины и др.), а также перспективны при построении новых криптографических алгоритмов, поскольку они легко реализуются при помощи современных вычислительных устройств.

Для иллюстрации рассмотрим модификацию блочного шифра IDEA, который базируется на чередовании трех различных групповых операций – побитового сложения, сложения по модулю 2^{16} и умножения по модулю $2^{16}+1$. Заменим в раундовом преобразовании этого алгоритма модульное умножение операцией модульного сложения. Получим модифицированный алгоритм, раундовое шифрующее преобразование которого будет использовать чередование рассмотренных групповых операций – модульного и побитового сложения. Согласно выводам, такой модифицированный алгоритм не будет стойким к атакам, которые базируются на гомоморфизмах. Применение операции модульного умножения в раундовом шифрующем преобразовании делает алгоритм IDEA стойким к известным на сегодняшний день атакам, в том числе и к атакам, которые базируются на гомоморфизмах и разностном криптоанализе.

Библиографические ссылки

1. *Шемякина О. В.* О перемешивающих свойствах операций в конечном поле // Восьмая общероссийская научная конференция «Математика и безопасность информационных технологий» (МаБИТ-09). Труды. Москва, 2010. Т. 2. С. 87–90.
2. *Ковальчук Л. В., Сиренко О. А.* Анализ перемешивающих свойств операций модульного и побитового сложения, определенных на одном носителе // Кибернетика и системный анализ. 2011. № 5. С. 83–97.
3. *Ковальчук Л. В., Сиренко О. А.* Анализ перемешивающих свойств операций в конечном кольце // XIV Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах». Сборник тезисов. Киев, 2011. С. 45–46.
4. *Погорелов Б. А., Пудовкина М. А.* Факторструктуры преобразований // Математические вопросы криптографии. 2012. Т. 3. Вып. 3. С. 81–104.