УДК 621.391:519.2:519.7

Л.В. КОВАЛЬЧУК, Н.В. ЛЫСЕНКО, Л.В. СКРЫПНИК

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

Аннотация. Получены результаты, характеризующие влияние операции поразрядного (модульного) сложения на множестве векторов над простым конечным полем на структуру факторгруппы 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, с одной стороны, стойкие к различным современным атакам, а с другой — просты и удобны в реализации. Поэтому возникает вопрос о нахождении такого набора операций на множестве p-ичных (p — простое число) векторов (открытых текстов), которые легко реализуются и программным, и аппаратным способом, при этом имеют хорошие перемешивающие свойства. Чередование операций с такими свойствами обеспечивает стойкость примитива к различным алгебраическим и статистическим атакам, что позволяет строить примитивы с простой и удобной для реализации структурой.

В работе [1] получены результаты, характеризующие перемешивающие свойства операций в конечном поле, и показано, что действие операции сложения (умножения) на элементы классов смежности относительно операции умножения (сложения) существенно разрушает структуру соответствующей факторгруппы, поэтому использование композиции этих операций при построении алгоритма шифрования делает его стойким к криптоанализу на основе гоммоморфизмов.

В работе [2], напротив, показано, что существует такое разбиение множества Z_{2^n} на непересекающиеся классы, для которого композиция операций модульного сложения и обращения незначительно разрушает его структуру.

В работах [3, 4] сделаны выводы, которые характеризуют перемешивающие свойства операций побитового и модульного сложения, заданных на одном носителе.

В работе [5] получены результаты относительно наличия нетривиальных факторструктур для определенных преобразований аддитивных групп, в частности, обобщен результат из [3, 4], касающийся существования инвариантных подгрупп аддитивной группы кольца Z_{2^n} и подпространств линейного пространства V_n. Однако в этих работах доказано только существование инвариантных подгрупп, но не определены вероятности попадания в различные классы смежности суммы элементов, принадлежащих классам смежности по неинвариантной подгруппе.

В настоящей статье обобщены результаты [3, 4] для операций поразрядного и модульного сложения. Показано, что в зависимости от выбора подгруппы в $V_n(p)$ операция 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.

© Л.В. Ковальчук, Н.В. Лысенко, Л.В Скрыпник, 2014

ВСПОМОГАТЕЛЬНЫЕ ОБОЗНАЧЕНИЯ И РЕЗУЛЬТАТЫ

При доказательстве основных результатов используем следующие обозначения и утверждения. Здесь и далее $(V_n(p),\oplus_p)$ — множество векторов длины n с операцией поразрядного сложения по модулю простого числа p, а $(Z_{p^n},+)$ — аддитивная группа кольца вычетов с операцией сложения по модулю p^n. Каждому целому числу $z \in Z_{p^n}$ поставим в соответствие вектор длины n, являющийся p-ичным представлением этого числа. Таким образом, отождествим множества Z_{p^n} и $V_n(p)$. Целое число и соответствующий ему p-ичный вектор обозначим одинаково.

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

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

Обозначение вида

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

используем для p-ичного 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.

Лемма 1. 1. Любое подмножество множества $V_n(p)$, имеющее структуру

$$\underbrace{\cdots}_{b_{k+1}\text{ разрядов}}\ \underbrace{0\ \cdots\ 0}_{a_k\text{ разрядов}}\ \underbrace{\cdots}_{b_k\text{ разрядов}}\ \ldots\ \underbrace{0\ \cdots\ 0}_{a_2\text{ разрядов}}\ \underbrace{\cdots}_{b_2\text{ разрядов}}\ \underbrace{0\ \cdots\ 0}_{a_1\text{ разрядов}}\ \underbrace{\cdots}_{b_1\text{ разрядов}},$$

где $\sum_{i=1}^{k} a_i + \sum_{i=1}^{k+1} b_i = n,\ a_i > 0,\ b_i > 0,$ при $i = 2, \ldots, k;\ b_1 \geq 0,\ b_{k+1} \geq 0,$ является подгруппой в $(V_n(p),\oplus_p)$;

2. Все подгруппы в $(Z_{p^n},+)$ имеют следующую структуру:

$$\underbrace{\cdots}_{n-k\text{ разрядов}}\ \underbrace{0\ \cdots\ 0}_{k\text{ разрядов}}\quad \text{для некоторого } k = 0, \ldots, n.$$

Справедливость п. 1 леммы очевидна, а справедливость п. 2 следует из того, что группа $(Z_{p^n},+)$ является циклической.

Лемма 2. Пусть:

а) случайные величины x и y независимы и равновероятно распределены на множестве $\{0, \ldots, a-1\},\ a \in N,$ тогда

$$1)\ P(x + y < a) = P(x + y \geq a - 1) = \frac{1}{2} + \frac{1}{2a};$$

$$2)\ P(x + y < a - 1) = P(x + y \geq a) = \frac{1}{2} - \frac{1}{2a};$$

б) случайные величины x и y независимы и равновероятно распределены на группе $(Z_{p^n},+),$ тогда

$$P(x > y) = \frac{1}{2} - \frac{1}{2p^n} = q_n;\ P(x \leq y) = \frac{1}{2} + \frac{1}{2p^n} = s_n.$$

Доказательство. По формуле полной вероятности имеем для первого утверждения п. а):

$$P(x+y<a)=\sum_{i=0}^{a-1}P(x+y<a\,/\,y=i)\cdot P(y=i)=\sum_{i=0}^{a-1}P(x<a-i)\cdot P(y=i)=$$

$$=\frac{1}{a}\sum_{i=0}^{a-1}P(x<a-i)=\frac{1}{a}\sum_{j=1}^{a}P(x<j)=\frac{1}{a}\sum_{j=1}^{a}\frac{j}{a}=\frac{1}{a^2}\cdot\frac{(a+1)\cdot a}{2}=\frac{a+1}{2a}=\frac{1}{2}+\frac{1}{2a}.$$

Аналогично для второго утверждения п. а) имеем

$$P(x+y<a-1)=\sum_{i=0}^{a-1}P(x+y<a-1/\,y=i)\cdot P(y=i)=\sum_{i=0}^{a-1}P(x<a-i-1)\cdot P(y=i)=$$

$$=\frac{1}{a}\sum_{i=0}^{a-1}P(x<a-i-1)=\frac{1}{a}\sum_{j=0}^{a-1}P(x<j)=\frac{1}{a}\sum_{j=1}^{a-1}P(x<j)=\frac{1}{a}\sum_{j=1}^{a-1}\frac{j}{a}=$$

$$=\frac{1}{a^2}\cdot\frac{(a-1)\cdot a}{2}=\frac{a-1}{2a}=\frac{1}{2}-\frac{1}{2a}.$$

Поскольку $P(x+y<a)=1-P(x+y\ge a)=\frac{1}{2}+\frac{1}{2a}$ и $P(x+y<a-1)=1-$ $-P(x+y\ge a-1)=\frac{1}{2}-\frac{1}{2a}$, то $P(x+y\ge a)=P(x+y<a-1)=\frac{1}{2}-\frac{1}{2a}$ и $P(x+y\ge$ $\ge a-1)=P(x+y<a)=\frac{1}{2}+\frac{1}{2a}$.

Докажем утверждения п. б): обозначим $s=P(x>y)$. Тогда $P(x=y)=$ $=\frac{p^n}{p^{2n}}=\frac{1}{p^n}$. Найдем s. Используем тот факт, что $P(x\le y)=1-P(x>y)$, отсюда $P(x<y)+P(x=y)=1-P(x>y)$.

Поскольку $P(x>y)=P(x<y)=s$, получим уравнение $s+\frac{1}{p^n}=1-s$, откуда $s=\frac{1}{2}-\frac{1}{2p^n}$. Тогда

$$P(x>y)=s=\frac{1}{2}-\frac{1}{2p^n},\ P(x\le y)=1-P(x>y)=1-s=1-\left(\frac{1}{2}-\frac{1}{2p^n}\right)=\frac{1}{2}+\frac{1}{2p^n}.$$

В приведенных обозначениях $P(x>y)=\frac{1}{2}-\frac{1}{2p^n}=q_n$, а $P(x\le y)=$ $=\frac{1}{2}+\frac{1}{2p^n}=s_n$.

Лемма доказана.

Замечание 1. Пусть на $(Z_{p^n},+)$ определены

$$A=\underbrace{A_m}_{l_m\text{ разрядов}}\ \underbrace{A_{m-1}}_{l_{m-1}\text{ разрядов}}\ \dots\ \underbrace{A_1}_{l_1\text{ разрядов}},$$

$$B=\underbrace{B_m}_{l_m\text{ разрядов}}\ \underbrace{B_{m-1}}_{l_{m-1}\text{ разрядов}}\ \dots\ \underbrace{B_1}_{l_1\text{ разрядов}},$$

где $0\le A_i,B_i<p^{l_i},\ i=1,\dots,m,\ \sum_{i=1}^{m}l_i=n$.

Рассмотрим сумму

$$C=A+B=\underbrace{C_m}_{l_m\text{ разрядов}}\ \underbrace{C_{m-1}}_{l_{m-1}\text{ разрядов}}\ \dots\ \underbrace{C_1}_{l_1\text{ разрядов}}.$$

Обозначим v_i, $i=1,\dots,m$, бит переноса из блока C_{i-1}:

$$v_1=0,\ v_i=\begin{cases}0, & \text{если } A_{i-1}+B_{i-1}+v_{i-1}<p^{l_{i-1}},\\ 1 & \text{в противном случае.}\end{cases}$$

Тогда очевидно, что $P(v_i=a_i/v_{i-1}=a_{i-1},\dots,v_1=a_1)=P(v_i=a_i/v_{i-1}=a_{i-1})$, где $a_i\in\{0,1\}$, $i=1,\dots,m$.

ВЛИЯНИЕ ОПЕРАЦИИ МОДУЛЬНОГО СЛОЖЕНИЯ НА СТРУКТУРУ ФАКТОРГРУППЫ $(V_n(p),\oplus_p)$ ПО ЕЕ ПОДГРУППЕ

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

$$\underbrace{\begin{matrix}B_{k+1}\\ \dots\end{matrix}}_{b_{k+1}\text{ разрядов}}\ \underbrace{\begin{matrix}A_k\\ 0\ \dots\ 0\end{matrix}}_{a_k\text{ разрядов}}\ \underbrace{\begin{matrix}B_k\\ \dots\end{matrix}}_{b_k\text{ разрядов}}\ \dots\ \underbrace{\begin{matrix}A_2\\ 0\ \dots\ 0\end{matrix}}_{a_2\text{ разрядов}}\ \underbrace{\begin{matrix}B_2\\ \dots\end{matrix}}_{b_2\text{ разрядов}}\ \underbrace{\begin{matrix}A_1\\ 0\ \dots\ 0\end{matrix}}_{a_1\text{ разрядов}}\ \underbrace{\begin{matrix}B_1\\ \dots\end{matrix}}_{b_1\text{ разрядов}},$$

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

Справедлива следующая теорема.

Теорема 1. Пусть $G=G(a_1,a_2,\dots,a_k,b_1,b_2,\dots,b_k,b_{k+1})$ — рассмотренная выше подгруппа индекса p^a группы $(V_n(p),\oplus_p)$, c и d — независимые случайные элементы, которые равновероятно распределены на классах смежности H_i и H_j по подгруппе G соответственно, $i,j=1,\dots,p^a$. Тогда имеем следующие утверждения.

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

2. Если $H_i=H_j$, то элементы классов смежности, в которые разность элементов c и d по модулю p^n попадает с ненулевой вероятностью, имеют вид

$$\underbrace{\begin{matrix}B_{k+1}\\ \dots\end{matrix}}_{b_{k+1}\text{ разрядов}}\ \underbrace{\begin{matrix}A_k\\ \dots\end{matrix}}_{a_k\text{ разрядов}}\ \underbrace{\begin{matrix}B_k\\ \dots\end{matrix}}_{b_k\text{ разрядов}}\ \dots\ \underbrace{\begin{matrix}A_1\\ \dots\end{matrix}}_{a_1\text{ разрядов}}\ \underbrace{\begin{matrix}B_1\\ \dots\end{matrix}}_{b_1\text{ разрядов}},$$

где блоки A_l содержат либо только нули, либо $p-1$ для любого $l=1,\dots,k$; количество указанных классов смежности равно 2^k, если $b_1>0$, и 2^{k-1}, если $b_1=0$; 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, если $b_1>0$, и p^a-2^{k-1}, если $b_1=0$.

Более того, 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 зависят только от вида подгруппы G.

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

Доказательство. 1. Пусть

$$c = \underbrace{\begin{matrix}B_{k+1}^c \\ \cdots\end{matrix}}_{b_{k+1}\text{ разрядов}} \underbrace{\begin{matrix}c_k \\ \cdots\end{matrix}}_{a_k\text{ разрядов}} \underbrace{\begin{matrix}B_k^c \\ \cdots\end{matrix}}_{b_k\text{ разрядов}} \ \ldots \ \underbrace{\begin{matrix}c_1 \\ \cdots\end{matrix}}_{a_1\text{ разрядов}} \underbrace{\begin{matrix}B_1^c \\ \cdots\end{matrix}}_{b_1\text{ разрядов}},$$

$$d = \underbrace{\begin{matrix}B_{k+1}^d \\ \cdots\end{matrix}}_{b_{k+1}\text{ разрядов}} \underbrace{\begin{matrix}d_k \\ \cdots\end{matrix}}_{a_k\text{ разрядов}} \underbrace{\begin{matrix}B_k^d \\ \cdots\end{matrix}}_{b_k\text{ разрядов}} \ \ldots \ \underbrace{\begin{matrix}d_1 \\ \cdots\end{matrix}}_{a_1\text{ разрядов}} \underbrace{\begin{matrix}B_1^d \\ \cdots\end{matrix}}_{b_1\text{ разрядов}},$$

где разряды из блоков $B_1^c, \ldots, B_{k+1}^c, B_1^d, \ldots, B_{k+1}^d$ могут принимать произвольные значения, а блоки $c_1, \ldots, c_k, d_1, \ldots, d_k$ являются фиксированными. Тогда

$$f = c + d = \underbrace{\begin{matrix}B_{k+1} \\ \cdots\end{matrix}}_{b_{k+1}\text{ разрядов}} \underbrace{\begin{matrix}F_k \\ \cdots\end{matrix}}_{a_k\text{ разрядов}} \underbrace{\begin{matrix}B_k \\ \cdots\end{matrix}}_{b_k\text{ разрядов}} \ \ldots \ \underbrace{\begin{matrix}F_1 \\ \cdots\end{matrix}}_{a_1\text{ разрядов}} \underbrace{\begin{matrix}B_1 \\ \cdots\end{matrix}}_{b_1\text{ разрядов}}, \quad (1)$$

где $F_i = \begin{cases} (c_i + d_i) \bmod p^{a_i}, & \text{если } B_i^c + B_i^d + z_i < p^{b_i},\ i = 1, \ldots, k, \\ (c_i + d_i + 1) \bmod p^{a_i} & \text{в противном случае,} \end{cases}$

z_i — бит переноса из блока F_{i-1}, $z_1 = 0$.

Используя результат п. а) леммы 2, получаем при $z_i = 0$:

$$F_i = \begin{cases} (c_i + d_i) \bmod p^{a_i} & \text{с вероятностью } s_{b_i} = \dfrac{1}{2} + \dfrac{1}{2p^{b_i}}, \\ (c_i + d_i + 1) \bmod p^{a_i} & \text{с вероятностью } q_{b_i} = \dfrac{1}{2} - \dfrac{1}{2p^{b_i}}, \end{cases}$$

а при $z_i = 1$ имеем

$$F_i = \begin{cases} (c_i + d_i) \bmod p^{a_i} & \text{с вероятностью } q_{b_i} = \dfrac{1}{2} - \dfrac{1}{2p^{b_i}}, \\ (c_i + d_i + 1) \bmod p^{a_i} & \text{с вероятностью } s_{b_i} = \dfrac{1}{2} + \dfrac{1}{2p^{b_i}}. \end{cases}$$

Вследствие замечания 1

$$P(F_k = f_k, F_{k-1} = f_{k-1}, \ldots, F_1 = f_1) = P(F_k = f_k / F_{k-1} = f_{k-1}),$$

где $f_i \in \{(c_i + d_i) \bmod p^{a_i}, (c_i + d_i + 1) \bmod p^{a_i}\}$, поскольку значение F_k полностью определяется битом переноса из предыдущих разрядов. Следовательно,

$$P\left(f = \underbrace{\begin{matrix}B_{k+1} \\ \cdots\end{matrix}}_{b_{k+1}\text{ разрядов}} \underbrace{\begin{matrix}f_k \\ \cdots\end{matrix}}_{a_k\text{ разрядов}} \underbrace{\begin{matrix}B_k \\ \cdots\end{matrix}}_{b_k\text{ разрядов}} \ \ldots \ \underbrace{\begin{matrix}f_1 \\ \cdots\end{matrix}}_{a_1\text{ разрядов}} \underbrace{\begin{matrix}B_1 \\ \cdots\end{matrix}}_{b_1\text{ разрядов}} \right) =$$

$$= P(F_k = f_k, F_{k-1} = f_{k-1}, \ldots, F_1 = f_1) = P(F_k = f_k / F_{k-1} = f_{k-1}, \ldots, F_1 = f_1) \times$$

$$\times P(F_{k-1} = f_{k-1} / F_{k-2} = f_{k-2}, \ldots, F_1 = f_1) \times \ldots \times P(F_2 = f_2 / F_1 = f_1) \times$$

$$\times P(F_1 = f_1) = P(F_k = f_k / F_{k-1} = f_{k-1}) \times P(F_{k-1} = f_{k-1} / F_{k-2} = f_{k-2}) \times \ldots$$

$$\ldots \times P(F_2 = f_2 / F_1 = f_1) \times P(F_1 = f_1) = u_k \times u_{k-1} \times \ldots \times u_2 \times u_1, \quad (2)$$

где

$$u_i = \begin{cases} s_{b_i} = \dfrac{1}{2} + \dfrac{1}{2p^{b_i}}, & \text{если } f_i = c_i + d_i, \\ q_{b_i} = \dfrac{1}{2} - \dfrac{1}{2p^{b_i}}, & \text{если } f_i = c_i + d + 1, \end{cases}$$

для $z_i = 0$,

$$u_i = \begin{cases} s_{b_i} = \dfrac{1}{2} + \dfrac{1}{2p^{b_i}}, & \text{если } f_i = c_i + d_i + 1, \\ q_{b_i} = \dfrac{1}{2} - \dfrac{1}{2p^{b_i}}, & \text{если } f_i = c_i + d, \end{cases}$$

для $z_i = 1$.

В случае $b_1 = 0$: $F_1 = c_1 + d_1$ с вероятностью 1 и $u_1 = 1$.

Из формулы (1) следует, что количество классов смежности по подгруппе G, в которые сумма элементов c и d по модулю p^n попадает с ненулевой вероятностью, равно 2^k, если $b_1 > 0$, и 2^{k-1}, если $b_1 = 0$, так как каждое F_i (кроме F_1) может принимать два значения; F_1 принимает одно значение, если $b_1 = 0$, и два значения, если $b_1 \neq 0$.

2. Докажем теперь утверждения для разности по модулю p^n элементов c и c', принадлежащих одному классу смежности. Вначале проведем доказательство для случая $b_1 > 0$.

Пусть

$$c = \underbrace{B_{k+1}^c \cdots}_{b_{k+1}\text{ разрядов}} \underbrace{c_k \cdots}_{a_k\text{ разрядов}} \underbrace{B_k^c \cdots}_{b_k\text{ разрядов}} \cdots \underbrace{c_1 \cdots}_{a_1\text{ разрядов}} \underbrace{B_1^c \cdots}_{b_1\text{ разрядов}},$$

$$c' = \underbrace{B_{k+1}^{c'} \cdots}_{b_{k+1}\text{ разрядов}} \underbrace{c_k \cdots}_{a_k\text{ разрядов}} \underbrace{B_k^{c'} \cdots}_{b_k\text{ разрядов}} \cdots \underbrace{c_1 \cdots}_{a_1\text{ разрядов}} \underbrace{B_1^{c'} \cdots}_{b_1\text{ разрядов}},$$

где разряды из блоков $B_1^c, \ldots, B_{k+1}^c, B_1^{c'}, \ldots, B_{k+1}^{c'}$ могут принимать произвольные значения, а блоки $c_1, \ldots, c_k$ являются фиксированными.

Тогда

$$e = c - c' = \underbrace{B_{k+1} \cdots}_{b_{k+1}\text{ разрядов}} \underbrace{E_k \cdots}_{a_k\text{ разрядов}} \underbrace{B_k \cdots}_{b_k\text{ разрядов}} \cdots \underbrace{E_1 \cdots}_{a_1\text{ разрядов}} \underbrace{B_1 \cdots}_{b_1\text{ разрядов}}, \qquad (3)$$

где $E_i = \begin{cases} \underbrace{0 \quad \cdots \quad 0}_{a_i\text{ разрядов}}, & \text{если } B_i^c - z_i \geq B_i^{c'},\ i = 1, \ldots, k, \\ \underbrace{p-1 \cdots\ p-1}_{a_i\text{ разрядов}} & \text{в противном случае,} \end{cases}$

z_i — бит заимствования для блока E_{i-1}, $z_1 = 0$.

Используя результат п. б) леммы 2, получаем при $z_i = 0$:

$$E_i = \begin{cases} \underbrace{0 \quad \cdots \quad 0}_{a_i\text{ разрядов}} & \text{с вероятностью } s_{b_i} = \dfrac{1}{2} + \dfrac{1}{2p^{b_i}}, \\ \underbrace{p-1 \cdots\ p-1}_{a_i\text{ разрядов}} & \text{с вероятностью } q_{b_i} = \dfrac{1}{2} - \dfrac{1}{2p^{b_i}}, \end{cases}$$

а при $z_i = 1$ имеем

$$E_i = \begin{cases} \underbrace{0 \quad \cdots \quad 0}_{a_i\text{ разрядов}} & \text{с вероятностью } q_{b_i} = \dfrac{1}{2} - \dfrac{1}{2p^{b_i}}, \\ \underbrace{p-1 \cdots\ p-1}_{a_i\text{ разрядов}} & \text{с вероятностью } s_{b_i} = \dfrac{1}{2} + \dfrac{1}{2p^{b_i}}. \end{cases}$$

Используем результаты, полученные при доказательстве утверждения для суммы элементов. Тогда

$$P\left(e=\underbrace{\overset{B_{k+1}}{\cdots}}_{b_{k+1}\text{ разрядов}}\ \underbrace{\overset{e_k}{\cdots}}_{a_k\text{ разрядов}}\ \underbrace{\overset{B_k}{\cdots}}_{b_k\text{ разрядов}}\ \ldots\ \underbrace{\overset{e_1}{\cdots}}_{a_1\text{ разрядов}}\ \underbrace{\overset{B_1}{\cdots}}_{b_1\text{ разрядов}}\right)=$$

$$=P(E_k=e_k,E_{k-1}=e_{k-1},\ldots,E_1=e_1)=P(E_k=e_k/E_{k-1}=e_{k-1})\times P(E_{k-1}=$$
$$=e_{k-1}/E_{k-2}=e_{k-2})\times\ldots\times P(E_2=e_2/E_1=e_1)\times P(E_1=e_1)=$$
$$=u_k\times u_{k-1}\times\ldots\times u_2\times u_1,$$

где

$$e_i\in\left\{\underbrace{0\ \cdots\ 0}_{a_i\text{ разрядов}},\ \underbrace{p-1\cdots\ p-1}_{a_i\text{ разрядов}}\right\},$$

$$u_i=\begin{cases}s_{b_i}=\dfrac{1}{2}+\dfrac{1}{2p^{b_i}}, & \text{если } e_i=\underbrace{0\ \cdots\ 0}_{a_i\text{ разрядов}},\\ q_{b_i}=\dfrac{1}{2}-\dfrac{1}{2p^{b_i}}, & \text{если } e_i=\underbrace{p-1\cdots\ p-1}_{a_i\text{ разрядов}},\end{cases}$$

для $z_i=0$,

$$u_i=\begin{cases}q_{b_i}=\dfrac{1}{2}-\dfrac{1}{2p^{b_i}}, & \text{если } e_i=\underbrace{0\ \cdots\ 0}_{a_i\text{ разрядов}},\\ s_{b_i}=\dfrac{1}{2}+\dfrac{1}{2p^{b_i}}, & \text{если } e_i=\underbrace{p-1\cdots\ p-1}_{a_i\text{ разрядов}},\end{cases}$$

для $z_i=1$.

В случае $b_1=0$: $E_1=\underbrace{0\ \cdots\ 0}_{a_1\text{ разрядов}}$ с вероятностью 1 и $u_1=1$.

Из формулы (3) следует, что количество классов смежности по подгруппе G, в которые разность элементов c и d по модулю p^n попадает с ненулевой вероятностью, равно 2^k, если $b_1>0$, и 2^{k-1}, если $b_1=0$, так как каждое E_i (кроме E_1) может принимать два значения; E_1 принимает одно значение, если $b_1=0$, и два значения, если $b_1\neq 0$.

3. Здесь утверждение непосредственно следует из формулы (2).

Теорема доказана.

Рассмотрим несколько примеров применения теоремы для подгрупп различной структуры.

Пример 1. Пусть $H_{t,m}$ — подгруппа $(V_n(3),\oplus_3)$ индекса 9, элементы которой имеют вид

$$\underbrace{\cdots}\ 0\ \underbrace{\cdots}_{m\text{ разрядов}}\ 0\ \underbrace{\cdots}_{t\text{ разрядов}}.$$

Рассмотрим действие операции модульного сложения в группе $(Z_{3^n},+)$ на элементы факторгруппы $(V_n(3),\oplus_3)$ по выбранной подгруппе $H_{t,m}$ относительно операции поразрядного сложения.

Выпишем все классы смежности по этой подгруппе:

$H_1=\underbrace{\cdots}\ 0\ \underbrace{\cdots}_{m\text{ разрядов}}\ 0\ \underbrace{\cdots}_{t\text{ разрядов}}$; $H_2=\underbrace{\cdots}\ 0\ \underbrace{\cdots}_{m\text{ разрядов}}\ 1\ \underbrace{\cdots}_{t\text{ разрядов}}$; $H_3=\underbrace{\cdots}\ 0\ \underbrace{\cdots}_{m\text{ разрядов}}\ 2\ \underbrace{\cdots}_{t\text{ разрядов}}$;

$H_4=\underbrace{\cdots}\ 1\ \underbrace{\cdots}_{m\text{ разрядов}}\ 0\ \underbrace{\cdots}_{t\text{ разрядов}}$; $H_5=\underbrace{\cdots}\ 1\ \underbrace{\cdots}_{m\text{ разрядов}}\ 1\ \underbrace{\cdots}_{t\text{ разрядов}}$; $H_6=\underbrace{\cdots}\ 1\ \underbrace{\cdots}_{m\text{ разрядов}}\ 2\ \underbrace{\cdots}_{t\text{ разрядов}}$;

$H_7=\underbrace{\cdots}\ 2\ \underbrace{\cdots}_{m\text{ разрядов}}\ 0\ \underbrace{\cdots}_{t\text{ разрядов}}$; $H_8=\underbrace{\cdots}\ 2\ \underbrace{\cdots}_{m\text{ разрядов}}\ 1\ \underbrace{\cdots}_{t\text{ разрядов}}$; $H_9=\underbrace{\cdots}\ 2\ \underbrace{\cdots}_{m\text{ разрядов}}\ 2\ \underbrace{\cdots}_{t\text{ разрядов}}$.

Тогда вероятности $P(v_1+v_2\in H_i / v_1\in H_j, v_2\in H_k)$, где $i, j, k=1,\dots,9$, описываются табл. 1, а вероятности $P(v_1-v_2\in H_i / v_1, v_2\in H_j)$, где $i, j, k=1,\dots,9$, — табл. 2. Отметим, что табл. 1 симметрична относительно главной диагонали.

Таблица 1. Вероятности попадания суммы векторов v_1 и v_2 в соответствующий класс смежности

v_2 \ v_1	H_1			H_2			…	H_9		
H_1	H_1 $s_t s_m$	H_2 $q_t s_m$	H_3 0	0	$s_t s_m$	$q_t s_m$	…	$q_t s_m$	0	$s_t q_m$
	H_4 $s_t q_m$	H_5 $q_t q_m$	H_6 0	0	$s_t q_m$	$q_t q_m$	…	0	0	0
	H_7 0	H_8 0	H_9 0	0	0	0	…	$q_t q_m$	0	$s_t s_m$
H_2	0	$s_t s_m$	$q_t s_m$	$q_t q_m$	0	$s_t s_m$	…	$s_t s_m$	$q_t s_m$	0
	0	$s_t q_m$	$q_t q_m$	$q_t s_m$	0	$s_t q_m$	…	0	0	0
	0	0	0	0	0	0	…	$s_t q_m$	$q_t q_m$	0
…	…			…			…	…		
H_9	$q_t s_m$	0	$s_t q_m$	$s_t s_m$	$q_t s_m$	0	…	0	0	0
	0	0	0	0	0	0	…	0	$s_t q_m$	$q_t q_m$
	$q_t q_m$	0	$s_t s_m$	$s_t q_m$	$q_t q_m$	0	…	0	$s_t s_m$	$q_t s_m$

Таблица 2. Вероятности попадания разности векторов v_1 и v_2 в соответствующий класс смежности

v_1, v_2 \ $v_1 - v_2$	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8	H_9
H_i, $i=1,\dots,9$	$s_t s_m$	0	$q_t q_m$	0	0	0	$s_t q_m$	0	$q_t s_m$

Пример 2. Пусть H_t — подгруппа $(V_n(3),\oplus_3)$ индекса 9, элементы которой имеют вид

$$\underbrace{\cdots}\ 0\ \underbrace{\cdots}_{t\text{ разрядов}}\ 0.$$

Выпишем все классы смежности по этой подгруппе:

$$H_1=\underbrace{\cdots}\ 0\ \underbrace{\cdots}_{t\text{ разрядов}}\ 0;\ H_2=\underbrace{\cdots}\ 0\ \underbrace{\cdots}_{t\text{ разрядов}}\ 1;\ H_3=\underbrace{\cdots}\ 0\ \underbrace{\cdots}_{t\text{ разрядов}}\ 2;$$

$$H_4=\underbrace{\cdots}\ 1\ \underbrace{\cdots}_{t\text{ разрядов}}\ 0;\ H_5=\underbrace{\cdots}\ 1\ \underbrace{\cdots}_{t\text{ разрядов}}\ 1;\ H_6=\underbrace{\cdots}\ 1\ \underbrace{\cdots}_{t\text{ разрядов}}\ 2;$$

$$H_7=\underbrace{\cdots}\ 2\ \underbrace{\cdots}_{t\text{ разрядов}}\ 0;\ H_8=\underbrace{\cdots}\ 2\ \underbrace{\cdots}_{t\text{ разрядов}}\ 1;\ H_9=\underbrace{\cdots}\ 2\ \underbrace{\cdots}_{t\text{ разрядов}}\ 2.$$

Рассмотрим действие операции модульного сложения в группе $(Z_{3^n},+)$ на элементы факторгруппы $(V_n(3),\oplus_3)$ по выбранной подгруппе H_t.

Тогда вероятности $P(v_1+v_2\in H_i / v_1\in H_j, v_2\in H_k)$, где $i, j, k=1,\dots,9$, описываются табл. 3, а вероятности $P(v_1-v_2\in H_i / v_1, v_2\in H_j)$, где $i, j, k=1,\dots,9$, — табл. 4. Отметим, что табл. 3 симметрична относительно главной диагонали.

Таблица 3. Вероятности попадания суммы векторов v_1 и v_2 в соответствующий класс смежности

v_2 \ v_1	H_1			H_2			…	H_9		
H_1	H_1 s_t	H_2 0	H_3 0	0	s_t	0	…	0	0	q_t
	H_4 q_t	H_5 0	H_6 0	0	q_t	0	…	0	0	0
	H_7 0	H_8 0	H_9 0	0	0	0	…	0	0	s_t
H_2	0	s_t	0	0	0	s_t	…	s_t	0	0
	0	q_t	0	0	0	q_t	…	0	0	0
	0	0	0	0	0	0	…	q_t	0	0
…	…			…			…	…		
H_9	0	0	q_t	s_t	0	0	…	0	0	0
	0	0	0	0	0	0	…	0	q_t	0
	0	0	s_t	q_t	0	0	…	0	s_t	0

Таблица 4. Вероятности попадания разности векторов v_1 и v_2 в соответствующий класс смежности

v_1, v_2 \ $v_1 - v_2$	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8	H_9
H_i, $i = 1, \ldots, 9$	s_t	0	0	0	0	0	q_t	0	0

Отметим, что если в подгруппе имеются только нулевые блоки единичной длины, то количество классов смежности, в которые сумма векторов по модулю p^n попадает с ненулевой вероятностью, является наибольшим; если нулевые блоки имеют большую длину, то количество классов смежности, в которые сумма векторов по модулю p^n попадает 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 $(Z_{p^n},+)$ ПО ЕЕ ПОДГРУППЕ ИНДЕКСА p^k ОТНОСИТЕЛЬНО МОДУЛЬНОГО СЛОЖЕНИЯ

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

a) G_k (в соответствующем представлении) — подгруппа $(V_n(p),\oplus_p)$;

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 $c-d \in G_k$, $0 \le i < p^k$;

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

Докажем каждое утверждение:

a) в соответствии с леммой 1 подгруппа G_k имеет структуру

$$\underbrace{\cdots}_{n-k \text{ разрядов}} \underbrace{0 \quad \cdots \quad 0}_{k \text{ разрядов}};$$

b) поскольку $i + 0 = i \oplus_p 0$, $0 \le i < p^k$, классы смежности по подгруппе G_k относительно операций $+$ и $\oplus_p$ совпадают и имеют вид

$$\underbrace{\begin{matrix} B \\ \cdots \end{matrix}}_{n-k \text{ разрядов}} \underbrace{\begin{matrix} A \\ \cdots \end{matrix}}_{k \text{ разрядов}},$$

где разряды из блока B могут принимать произвольные значения, а блок A является фиксированным.

Пусть $c \in i + G_k\,(i \oplus_p G_k)$, $d \in j + G_k\,(j \oplus_p G_k)$, тогда

$$c = \underbrace{\begin{matrix} B_c \\ \cdots \end{matrix}}_{n-k \text{ разрядов}} \underbrace{\begin{matrix} i \\ \cdots \end{matrix}}_{k \text{ разрядов}}, \quad d = \underbrace{\begin{matrix} B_d \\ \cdots \end{matrix}}_{n-k \text{ разрядов}} \underbrace{\begin{matrix} j \\ \cdots \end{matrix}}_{k \text{ разрядов}},$$

где разряды из блоков B_c, B_d могут принимать произвольные значения, а блоки i, j являются фиксированными;

c) если c и d принадлежат одному классу смежности по подгруппе G_k, т.е. $i = j$, тогда

$$f = c - d = \underbrace{\begin{matrix} B \\ \cdots \end{matrix}}_{n-k \text{ разрядов}} \underbrace{0 \quad \begin{matrix} A \\ \cdots \end{matrix} \quad 0}_{k \text{ разрядов}},$$

так как $i - j = i - i = 0$;

d) для любых c и d имеем

$$f = c \oplus_p d = \underbrace{\begin{matrix} B_1 \\ \cdots \end{matrix}}_{n-k \text{ разрядов}} \underbrace{\begin{matrix} A_1 \\ \cdots \end{matrix}}_{k \text{ разрядов}},$$

где $A_1 = i \oplus_p j$;

e) для любых c и d имеем

$$f = c + d = \underbrace{\begin{matrix} B_1 \\ \cdots \end{matrix}}_{n-k \text{ разрядов}} \underbrace{\begin{matrix} A_1 \\ \cdots \end{matrix}}_{k \text{ разрядов}},$$

где $A_1 = (i + j) \bmod p^k$.

Теорема доказана.

Из данной теоремы можно сделать следующий вывод: если подгруппа имеет структуру, описанную в п. б) леммы 1, т.е. для некоторого $k = 0, \ldots, n$ элементы этой подгруппы имеют вид

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

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

ЗАКЛЮЧЕНИЕ

Результаты, полученные в данной работе, характеризуют перемешивающие свойства операций поразрядного и модульного сложения, заданных на одном носителе. Наиболее интересным является тот факт, что действие операции модульного сложения на факторгруппу относительно операции поразрядного

сложения существенно зависит от выбора подгруппы в $(V_n(p),\oplus_p)$, а операция поразрядного сложения всегда сохраняет структуру соответствующей факторгруппы по любой подгруппе группы $(Z_{p^n},+)$.

Другими словами, полученные результаты свидетельствуют о плохих перемешивающих свойствах рассмотренных операций: во-первых, существует много нетривиальных подгрупп, которые являются подгруппами относительно обеих операций; во-вторых, для таких подгрупп полностью сохраняется структура соответствующей факторгруппы. В терминах атак, базирующихся на гомоморфизмах [6], можно утверждать, что классы смежности по таким подгруппам создают блоки импримитивности, а наличие таких блоков дает потенциальную возможность реализовать указанные атаки на блочные шифры, построенные с использованием только операций поразрядного и модульного сложения.

Рассмотренные операции используются в некоторых современных алгоритмах шифрования (IDEA (International Data Encryption Algorithm) [7] — международный алгоритм шифрования данных; ГОСТ 28147-89 [8] — действующий стандарт шифрования в Украине, России и некоторых других странах; «Калина» [9] — претендент на национальный стандарт шифрования Украины и др.), они перспективны при построении новых криптографических алгоритмов, поскольку легко реализуются с помощью современных вычислительных устройств.

СПИСОК ЛИТЕРАТУРЫ

1. Шемякина О.В. О перемешивающих свойствах операций в конечном поле // Тр. V Междунар. науч. конф. по проблемам безопасности и противодействия терроризму. Т. 2. Тр. VIII Общеросс. науч. конф. «Математика и безопасность информационных технологий» (МаБИТ, М., 2–30 окт. 2009 г.). — М.: МЦНМО, 2010. — **2**. — С. 87–90.
2. Шемякина О.В. О применении разбиения специального вида при исследовании операции обращения в конечном поле // Тр.VI Междунар. науч. конф. по проблемам безопасности и противодействия терроризму. Т. 2. Тр. IX общеросс. науч. конф. «Математика и безопасность информационных технологий» (МаБИТ, М., 11–12 нояб., 2010 г.). — М.: МЦНМО, 2010. — **2**. — С. 102–106.
3. 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.
4. Ковальчук Л.В., Сиренко О.А. Анализ перемешивающих свойств операций в конечном кольце // Тез. докл. XIV Междунар. науч.-практ. конф. «Безопасность информации в информационно-телекоммуникационных системах» (Киев, 17–20 мая 2011 г.) — Киев: НОЦ «Тезис» НТУУ «КПИ». — С. 45–46.
5. Погорелов Б.А., Пудовкина М.А. Факторструктуры преобразований // Математические вопросы криптографии — 2012. — **3**, вып. 3. — С. 81–104.
6. Paterson K.G. Imprimitive permutation groups and trapdoors in iterated block ciphers // Fast Software Encryption. — FSE'99, Proc. — Berlin: Springer Verlag, 1999. — P. 201–214.
7. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Advances in Cryptology — EUROCRYPT'91, Proc. — Berlin: Springer Verlag, 1991. — P 17–38.
8. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — Введен 01.07.1990. — М.: Госстандарт СССР, 1989. — С. 28.
9. Горбенко І.Д., Тоцький О.С., Казьміна С.В. Перспективний блоковий шифр «Калина» — основні положення та специфікація // Прикладна радіоелектроніка. — 2007 — **6**, № 2. — С. 195–208.

Поступила 02.07.2013

Key words: ring, factorgroup, mixing properties of operation, modular addition operations, operation of component addition.