УДК 621.391:519.2:519.7

Л.В. КОВАЛЬЧУК, О.А. СИРЕНКО

АНАЛИЗ ПЕРЕМЕШИВАЮЩИХ СВОЙСТВ ОПЕРАЦИЙ МОДУЛЬНОГО И ПОБИТОВОГО СЛОЖЕНИЯ, ОПРЕДЕЛЕННЫХ НА ОДНОМ НОСИТЕЛЕ

Ключевые слова: *кольцо вычетов, фактор-группа, алгебраические и статистические атаки, перемешивающие свойства операций.*

ВВЕДЕНИЕ

Одной из задач современной прикладной криптографии является создание криптографических примитивов, стойких к различным атакам, но простых и удобных в реализации. В связи с этим возникает вопрос о нахождении такого набора операций на множестве битовых векторов (открытых текстов), которые, с одной стороны, легко реализуются и программным, и аппаратным способом, а с другой — обладают «хорошими перемешивающими свойствами» [1–3]. Чередование операций с такими свойствами обеспечивает стойкость примитива к различным алгебраическим и статистическим атакам, что позволяет строить примитивы с простой и удобной в реализации структурой.

В работе [1] рассматривалось действие операции сложения (умножения) в конечном поле на смежные классы относительно умножения (сложения). Было показано, что действие операции сложения (умножения) на элементы классов смежности относительно операции умножения (сложения) существенно разрушает структуру соответствующей фактор-группы. Исходя из полученных результатов, в указанной работе сделан вывод о том, что применение композиции этих операций при построении алгоритма шифрования делает его стойким к криптоанализу на основе гомоморфизмов [1–3]. Однако в современных алгоритмах шифрования (например, [4–6, 8]) гораздо чаще используется композиция других операций, а именно операций модульного и побитового сложения. Поэтому не менее актуальна и интересна задача исследования перемешивающих свойств групповых операций побитового и модульного сложения, носителем которых является множество двоичных векторов. Такие свойства алгебраических операций характеризируют также стойкость шифров к атакам дифференциального криптоанализа [7, 8].

В данной статье исследуются вопросы, аналогичные рассмотренным в работах [1, 9]. Приводятся результаты, характеризующие перемешивающие свойства операций побитового и модульного сложения. Показано, что в зависимости от выбора подгруппы в $(V_n, \oplus)$ операция модульного сложения в $(\mathbb{Z}_{2^n}, +)$ может как существенно разрушать структуру фактор-группы по выбранной подгруппе, так и полностью ее сохранять. Также отмечено, что для любой подгруппы в $(\mathbb{Z}_{2^n}, +)$ операция побитового сложения всегда сохраняет структуру соответствующей фактор-группы.

ВСПОМОГАТЕЛЬНЫЕ ОБОЗНАЧЕНИЯ И РЕЗУЛЬТАТЫ

При доказательстве основных результатов используются следующие обозначения и утверждения. Здесь и далее под $(V_n, \oplus)$ будем понимать множество векторов длины n с операцией побитового сложения, а под $(\mathbb{Z}_{2^n}, +)$ — аддитив-

ную группу кольца вычетов $\mathbb{Z}_{2^n}$. Каждому целому числу $z \in \mathbb{Z}_{2^n}$ поставим в соответствие битовый вектор длины n, являющийся двоичным представлением этого числа. Таким образом, множества $\mathbb{Z}_{2^n}$ и V_n отождествлены. Целое число и соответствующий ему двоичный вектор обозначим одинаково; из контекста будет понятно, какое именно представление используется.

Для любого $t \geq 0$ введем следующие обозначения: $p_t = \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)$; $q_t = 1 - p_t$.

Обозначение вида

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

используется для битового вектора длины $n = \sum_{i=1}^{k} a_i + \sum_{i=1}^{k+1} b_i$, у которого слева имеется b_{k+1} произвольных битов, далее a_k нулевых битов и т.д.

Лемма 1. В указанных обозначениях:

а) все подгруппы в $(V_n, \oplus)$ имеют структуру

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

где $\sum_{i=1}^{k} a_i + \sum_{i=1}^{k+1} b_i = n$, $a_i > 0$, $b_i > 0$ при $i = 2, \ldots, k$; $b_1 \geq 0$, $a_1 > 0$, $b_{k+1} \geq 0$;

б) все подгруппы в $(\mathbb{Z}_{2^n}, +)$ имеют структуру

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

для некоторого $k = 0, \ldots, n$.

Лемма 2. 1. Пусть случайные величины x и y равновероятно распределены на множестве $\{0, \ldots, a-1\}$, $a \in \mathbb{Z}$. Тогда

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

2. Пусть случайные величины x и y равновероятно распределены на группе $(\mathbb{Z}_{2^n}, +)$. Тогда

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

Доказательство. 1. По формуле полной вероятности

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

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

Аналогично докажем второе утверждение п. 1:

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

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

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

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

2. Обозначим $p=P(x>y)$. Тогда $P(x=y)=\frac{2^n}{2^{2n}}=\frac{1}{2^n}$. Найдем p. Используем тот факт, что $P(x\le y)=1-P(x>y)$, тогда

$$P(x<y)+P(x=y)=1-P(x>y).$$

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

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

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

В принятых обозначениях $P(x>y)=\frac{1}{2}-\frac{1}{2^{n+1}}=q_n$, а $P(x\le y)=\frac{1}{2}+\frac{1}{2^{n+1}}=$ $=p_n$. Лемма доказана.

ВЛИЯНИЕ ОПЕРАЦИИ МОДУЛЬНОГО СЛОЖЕНИЯ НА СТРУКТУРУ ФАКТОР-ГРУППЫ $(V_n,\oplus)$ ПО ЕЕ ПОДГРУППЕ

Определение 1. Обозначим $G(a_1,a_2,\ldots,a_k;b_1,b_2,\ldots,b_k,b_{k+1})$ подгруппу индекса 2^a группы $(V_n,\oplus)$, элементы которой содержат k «нулевых» блоков $A_1,\ldots,A_k$, т.е. имеют следующую структуру:

$$\underbrace{\text{блок } B_{k+1}}_{\ldots}\ \underbrace{\text{блок } A_k}_{0\ \ldots\ 0}\ \underbrace{\text{блок } B_k}_{\ldots}\ \ldots\ \underbrace{\text{блок } A_2}_{0\ \ldots\ 0}\ \underbrace{\text{блок } B_2}_{\ldots}\ \underbrace{\text{блок } A_1}_{0\ \ldots\ 0}\ \underbrace{\text{блок } B_1}_{\ldots},$$

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

где биты из «ненулевых» блоков $B_1,\ldots,B_{k+1}$ 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 $i=2,\ldots,k$; $b_1\ge 0$, $a_1>0$, $b_{k+1}\ge 0$.

Теорема 1. Пусть $G(a_1, a_2, \ldots, a_k; b_1, b_2, \ldots, b_k, b_{k+1})$ — некоторая подгруппа индекса 2^a группы $(V_n, \oplus)$; v_1 и v_2 — случайные элементы, равновероятно распределенные в классах смежности H_i и H_j подгруппы G соответственно; $i, j = 1, \ldots, 2^a$. Тогда:

1) количество классов смежности по подгруппе G, в которые сумма элементов v_1 и v_2 по модулю 2^n попадает с ненулевой вероятностью, равно 2^k, если $b_1 > 0$; 2^{k-1}, если $b_1 = 0$, а количество классов смежности, в которые сумма элементов v_1 и v_2 по модулю 2^n попадает с нулевой вероятностью, равно $2^a - 2^k$, если $b_1 > 0$; $2^a - 2^{k-1}$, если $b_1 = 0$;

2) если $H_i = H_j$, то классы смежности, в которые разность элементов v_1 и v_2 по модулю 2^n попадает с ненулевой вероятностью, имеют вид

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

где блоки A_l содержат либо только 0, либо 1 для любого $l = 1, \ldots, k$, и количество этих классов смежности равно 2^k, если $b_1 > 0$; 2^{k-1}, если $b_1 = 0$, а количество классов смежности, в которые разность элементов v_1 и v_2 по модулю 2^n попадает с нулевой вероятностью, равно $2^a - 2^k$, если $b_1 > 0$; $2^a - 2^{k-1}$, если $b_1 = 0$. При этом вероятности попадания разности элементов v_1 и v_2 в различные классы смежности одинаковы при любом выборе класса смежности H_i (т.е. класса смежности, которому принадлежат v_1 и v_2) и зависят только от вида подгруппы, по которой строятся эти классы смежности;

3) ненулевые вероятности попадания суммы (разности) элементов v_1 и v_2 по модулю 2^n в соответствующие классы смежности находятся в пределах от $\prod_{i=1}^{k} q_{b_i}$ до $\prod_{i=1}^{k} p_{b_i}$.

Доказательство. Для доказательства данной теоремы достаточно рассмотреть подгруппу, содержащую один нулевой блок единичной длины и один нулевой блок большей длины. Выберем подгруппу $H_{t,m}$ группы $(V_n, \oplus)$ таким образом, что ее элементы имеют следующий вид:

$$\underbrace{\ldots}\ 00\ \underbrace{\ldots}_{m\text{ бит}}\ 0\ \underbrace{\ldots}_{t\text{ бит}}.$$

Рассмотрим действие операции модульного сложения в группе $\mathbb{Z}_{2^n}$ на элементы фактор-группы группы $(V_n, \oplus)$ по выбранной подгруппе $H_{t,m}$ индекса 8 относительно операции побитового сложения. Для этого выпишем все классы смежности по этой подгруппе:

$$H_1 = \underbrace{\ldots}\ 00\ \underbrace{\ldots}_{m\ \text{бит}}\ 0\ \underbrace{\ldots}_{t\ \text{бит}}; \qquad H_5 = \underbrace{\ldots}\ 01\ \underbrace{\ldots}\ 0\ \underbrace{\ldots};$$

$$H_2 = \underbrace{\ldots}\ 00\ \underbrace{\ldots}\ 1\ \underbrace{\ldots}; \qquad H_6 = \underbrace{\ldots}\ 01\ \underbrace{\ldots}\ 1\ \underbrace{\ldots};$$

$$H_3 = \underbrace{\ldots}\ 10\ \underbrace{\ldots}\ 0\ \underbrace{\ldots}; \qquad H_7 = \underbrace{\ldots}\ 11\ \underbrace{\ldots}\ 0\ \underbrace{\ldots};$$

$$H_4 = \underbrace{\ldots}\ 10\ \underbrace{\ldots}\ 1\ \underbrace{\ldots}; \qquad H_8 = \underbrace{\ldots}\ 11\ \underbrace{\ldots}\ 1\ \underbrace{\ldots}.$$

Тогда вероятности $P(v_1 + v_2 \in H_i \,/\, v_1 \in H_i\ ;\ v_2 \in H_k)$, где $i, j, k = 1,\ldots,8$, описываются табл. 1, симметричной относительно главной диагонали, а вероятности $P(v_1 - v_2 \in H_i \,/\, v_1, v_2 \in H_j)$, где $i, j = 1,\ldots,8$, описываются табл. 2.

Докажем сначала результаты табл. 1. Рассмотрим для примера доказательство некоторых возможных случаев, поскольку доказательство остальных случаев проводится аналогично.

Для произвольного вектора $v \in V_n$ введем обозначения

$$v = \underbrace{\ldots}\ 00\ \underbrace{\overbrace{\ldots}^{v^C}}_{m\ \text{бит}}\ 0\ \underbrace{\overbrace{\ldots}^{v^R}}_{t\ \text{бит}};$$

$$v' = 0\ \underbrace{\overbrace{\ldots}^{v^C}}_{m\ \text{бит}}\ 0\ \underbrace{\overbrace{\ldots}^{v^R}}_{t\ \text{бит}}.$$

1. Пусть $v_1 \in H_1, v_2 \in H_1$, тогда векторы v_1 и v_2 имеют следующий вид:

$$v_1 = \underbrace{\ldots}\ 00\ \underbrace{\ldots}_{m\ \text{бит}}\ 0\ \underbrace{\ldots}_{t\ \text{бит}}; \qquad v_2 = \underbrace{\ldots}\ 00\ \underbrace{\ldots}_{m\ \text{бит}}\ 0\ \underbrace{\ldots}_{t\ \text{бит}}.$$

По формуле полной вероятности имеем

$$P(v_1 + v_2 \in H_1) = P(v_1^R + v_2^R < 2^t \cap v_1' + v_2' < 2^{m+t+1}) =$$

$$= P(v_1' + v_2' < 2^{m+t+1} \,/\, v_1^R + v_2^R < 2^t) P(v_1^R + v_2^R < 2^t) =$$

$$= P(v_1^R + v_2^R < 2^t)\, P(v_1^C + v_2^C < 2^m).$$

Используя результат п. 1 леммы 2, получаем

$$P(v_1 + v_2 \in H_1) = \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} + \frac{1}{2^{m+1}}\right) = p_t\, p_m\ .$$

Таблица 1. Вероятности попадания суммы векторов v_1 и v_2 в соответствующий класс смежности H_i, $i = 1, \ldots, 8$

	$v_2 \in H_1$		$v_2 \in H_2$		$v_2 \in H_3$		$v_2 \in H_4$		$v_2 \in H_5$		$v_2 \in H_6$		$v_2 \in H_7$		$v_2 \in H_8$	
$v_1 \in H_1$	H_1 $p_t p_m$	H_2 $q_t p_m$	$q_t q_m$	$p_t p_m$	0	0	0	0	0	0	0	0	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$
	H_3 0	H_4 0	0	0	$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$	0	0	0	0
	H_5 $p_t q_m$	H_6 $q_t q_m$	$q_t p_m$	$p_t q_m$	0	0	0	0	$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$	0	0	0	0
	H_7 0	H_8 0	0	0	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$	0	0	0	0	$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$
$v_1 \in H_2$			$p_t q_m$	$q_t q_m$	0	0	0	0	0	0	0	0	$q_t p_m$	$p_t q_m$	$p_t p_m$	$q_t p_m$
			0	0	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t p_m$	$p_t q_m$	$q_t p_m$	0	0	0	0
			$p_t p_m$	$q_t p_m$	0	0	0	0	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$	0	0	0	0
			0	0	$q_t p_m$	$p_t q_m$	$p_t p_m$	$q_t p_m$	0	0	0	0	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$
$v_1 \in H_3$					$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$	0	0	0	0
					0	0	0	0	0	0	0	0	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$
					$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$	0	0	0	0	$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$
					0	0	0	0	$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$	0	0	0	0
$v_1 \in H_4$							$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t p_m$	$p_t p_m$	$q_t p_m$	0	0	0	0
							0	0	0	0	0	0	$q_t p_m$	$p_t q_m$	$p_t p_m$	$q_t p_m$
							$p_t p_m$	$q_t p_m$	0	0	0	0	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$
							0	0	$q_t q_m$	$p_t q_m$	$p_t q_m$	$q_t q_m$	0	0	0	0
$v_1 \in H_5$									0	0	0	0	$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$
									$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t q_m$	0	0	0	0
									0	0	0	0	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$
									$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$	0	0	0	0
$v_1 \in H_6$											0	0	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$
											$p_t q_m$	$q_t q_m$	0	0	0	0
											0	0	$q_t p_m$	$p_t q_m$	$p_t p_m$	$q_t p_m$
											$p_t p_m$	$q_t p_m$	0	0	0	0
$v_1 \in H_7$													0	0	0	0
													$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$
													0	0	0	0
													$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$
$v_1 \in H_8$															0	0
															$p_t q_m$	$q_t q_m$
															0	0
															$p_t p_m$	$q_t p_m$

Таблица 2. Вероятности попадания разности векторов v_1 и v_2 в соответствующий класс смежности H_i, $i = 1, \ldots, 8$

$v_1, v_2 \in H_i$	Вероятности попадания в H_i							
	H_1	H_2	H_3	H_4	H_5	H_6	H_7	H_8
H_i, $i = 1, \ldots, 8$	$p_t p_m$	$q_t q_m$	0	0	0	0	$p_t q_m$	$q_t p_m$

Аналогично найдем вероятности попадания в другие классы смежности:

$$P(v_1 + v_2 \in H_2) = P(v_1^R + v_2^R \geq 2^t)\, P(v_1^C + v_2^C < 2^m) =$$
$$= \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} + \frac{1}{2^{m+1}}\right) = q_t\, p_m\ ;$$

$$P(v_1 + v_2 \in H_3) = 0;$$

$$P(v_1 + v_2 \in H_4) = 0;$$

$$P(v_1 + v_2 \in H_5) = P(v_1^R + v_2^R < 2^t)\, P(v_1^C + v_2^C \geq 2^m) =$$
$$= \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{m+1}}\right) = p_t\ q_m\ ;$$

$$P(v_1 + v_2 \in H_6) = P(v_1^R + v_2^R \geq 2^t)\, P(v_1^C + v_2^C \geq 2^m) =$$
$$= \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{m+1}}\right) = q_t\ q_m\ ;$$

$$P(v_1 + v_2 \in H_7) = 0;$$

$$P(v_1 + v_2 \in H_8) = 0.$$

2. Пусть $v_1 \in H_5, v_2 \in H_5$, тогда векторы v_1 и v_2 имеют следующий вид:

$$v_1 = \underbrace{\ldots}\ 01\ \underbrace{\ldots}_{m\ \text{бит}}\ 0\ \underbrace{\ldots}_{t\,\text{бит}}\ ; \qquad v_2 = \underbrace{\ldots}\ 01\ \underbrace{\ldots}_{m\ \text{бит}}\ 0\ \underbrace{\ldots}_{t\,\text{бит}}\ .$$

Выполняя вычисления, аналогичные предыдущим, получим:

$$P(v_1 + v_2 \in H_1) = 0;$$

$$P(v_1 + v_2 \in H_2) = 0;$$

$$P(v_1 + v_2 \in H_3) = P(v_1^R + v_2^R < 2^t)\, P(v_1^C + v_2^C < 2^m) =$$
$$= \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} + \frac{1}{2^{m+1}}\right) = p_t\ p_m\ ;$$

$$P(v_1 + v_2 \in H_4) = P(v_1^R + v_2^R \geq 2^t)\, P(v_1^C + v_2^C < 2^m) =$$
$$= \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} + \frac{1}{2^{m+1}}\right) = q_t\ p_m\ ;$$

$$P(v_1 + v_2 \in H_5) = 0;$$

$$P(v_1 + v_2 \in H_6) = 0;$$

$$P(v_1 + v_2 \in H_7) = P(v_1^R + v_2^R < 2^t)\, P(v_1^C + v_2^C \geq 2^m) =$$
$$= \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{m+1}}\right) = p_t\ q_m\ ;$$

$$P(v_1 + v_2 \in H_8) = P(v_1^R + v_2^R \geq 2^t)\, P(v_1^C + v_2^C \geq 2^m) =$$
$$= \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{m+1}}\right) = q_t\ q_m\ .$$

3. Пусть $v_1 \in H_2$, $v_2 \in H_6$, тогда векторы v_1 и v_2 имеют вид

$$v_1 = \underbrace{\ldots}\ 00\ \underbrace{\ldots}_{m\ \text{бит}}\ 1\ \underbrace{\ldots}_{t\,\text{бит}}\ ; \qquad v_2 = \underbrace{\ldots}\ 01\ \underbrace{\ldots}_{m\ \text{бит}}\ 1\ \underbrace{\ldots}_{t\,\text{бит}}\ .$$

Получим следующие величины для соответствующих вероятностей:

$P(v_1 + v_2 \in H_1) = 0$;

$P(v_1 + v_2 \in H_2) = 0$;

$$P(v_1 + v_2 \in H_3) = P(v_1^R + v_2^R < 2^t)\, P(v_1^C + v_2^C + 1 \geq 2^m) =$$

$$= \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} + \frac{1}{2^{m+1}}\right) = p_t\, p_m\ ;$$

$$P(v_1 + v_2 \in H_4) = P(v_1^R + v_2^R \geq 2^t)\, P(v_1^C + v_2^C + 1 \geq 2^m) =$$

$$= \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} + \frac{1}{2^{m+1}}\right) = q_t\, p_m\ ;$$

$$P(v_1 + v_2 \in H_5) = P(v_1^R + v_2^R < 2^t) P(v_1^C + v_2^C + 1 < 2^m) =$$

$$= \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{m+1}}\right) = p_t q_m\ ;$$

$$P(v_1 + v_2 \in H_6) = P(v_1^R + v_2^R \geq 2^t)\, P(v_1^C + v_2^C + 1 < 2^m) =$$

$$= \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{m+1}}\right) = q_t q_m\ ;$$

$P(v_1 + v_2 \in H_7) = 0$;

$P(v_1 + v_2 \in H_8) = 0$.

4. Пусть $v_1 \in H_2$, $v_2 \in H_8$, тогда векторы v_1 и v_2 имеют вид

$$v_1 = \underbrace{\ldots}\ 00\ \underbrace{\ldots}_{m\ \text{бит}}\ 1\ \underbrace{\ldots}_{t\,\text{бит}}\ ; \qquad v_2 = \underbrace{\ldots}\ 11\ \underbrace{\ldots}_{m\ \text{бит}}\ 1\ \underbrace{\ldots}_{t\,\text{бит}}\ .$$

Получим следующие величины:

$$P(v_1 + v_2 \in H_1) = P(v_1^R + v_2^R < 2^t)\, P(v_1^C + v_2^C + 1 \geq 2^m) =$$

$$= \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} + \frac{1}{2^{m+1}}\right) = p_t\ p_m\ ;$$

$$P(v_1 + v_2 \in H_2) = P(v_1^R + v_2^R \geq 2^t)\, P(v_1^C + v_2^C + 1 \geq 2^m) =$$

$$= \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} + \frac{1}{2^{m+1}}\right) = q_t\ p_m\ ;$$

$P(v_1 + v_2 \in H_3) = 0$;

$P(v_1 + v_2 \in H_4) = 0$;

$P(v_1 + v_2 \in H_5) = 0$;

$P(v_1 + v_2 \in H_6) = 0$;

$$P(v_1 + v_2 \in H_7) = P(v_1^R + v_2^R < 2^t)\, P(v_1^C + v_2^C + 1 < 2^m) =$$

$$= \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{m+1}}\right) = p_t q_m;$$

$$P(v_1 + v_2 \in H_8) = P(v_1^R + v_2^R \geq 2^t)\, P(v_1^C + v_2^C + 1 < 2^m) =$$
$$= \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{m+1}}\right) = q_t q_m \ .$$

Докажем теперь результаты табл. 2. Для примера рассмотрим случай, когда $v_1 \in H_1, v_2 \in H_1$. Тогда эти векторы имеют вид

$$v_1 = \underbrace{\ldots}\ 00\ \underbrace{\ldots}_{m\ \text{бит}}\ 0\ \underbrace{\ldots}_{t\,\text{бит}}; \quad v_2 = \underbrace{\ldots}\ 00\ \underbrace{\ldots}_{m\ \text{бит}}\ 0\ \underbrace{\ldots}_{t\,\text{бит}}.$$

По формуле полной вероятности имеем

$$P(v_1 - v_2 \in H_{t,m}) = P(v_2^R \leq v_1^R \cap v_2' \leq v_1') = P(v_2' \leq v_1' / v_2^R \leq v_1^R)\, P(v_2^R \leq v_1^R) =$$
$$= P(v_2^R \leq v_1^R)\, P(v_2^C \leq v_1^C) \, .$$

Используя результат п. 2 леммы 2, получаем

$$P(v_1 - v_2 \in H_1) = \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} + \frac{1}{2^{m+1}}\right) = p_t p_m \ .$$

Аналогично для всех других вероятностей получим следующие значения:

$$P(v_1 - v_2 \in H_2) = P(v_1^C - 1 \geq v_2^C)\, P(v_1^R < v_2^R) = \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{m+1}}\right) = q_t q_m \ ;$$
$$P(v_1 - v_2 \in H_3) = 0 \, ;$$
$$P(v_1 - v_2 \in H_4) = 0 \, ;$$
$$P(v_1 - v_2 \in H_5) = 0 \, ;$$
$$P(v_1 - v_2 \in H_6) = 0 \, ;$$
$$P(v_1 - v_2 \in H_7) = P(v_1^R \geq v_2^R)\, P(v_1^C < v_2^C) = \left(\frac{1}{2} + \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} - \frac{1}{2^{m+1}}\right) = p_t q_m \, ;$$
$$P(v_1 - v_2 \in H_8) = P(v_1^R < v_2^R)\, P(v_1^C - 1 < v_2^C) = \left(\frac{1}{2} - \frac{1}{2^{t+1}}\right)\left(\frac{1}{2} + \frac{1}{2^{m+1}}\right) = q_t p_m \, .$$

Теорема доказана.

Рассмотрим несколько примеров применения теоремы для подгрупп разной структуры.

Пример 1. Пусть $H_{t,m}$ — подгруппа $(V_n, \oplus)$, индекс которой равен четырем, а ее элементы имеют следующий вид:

$$\underbrace{\ldots}\ 0\ \underbrace{\ldots}_{m\ \text{бит}}\ 0\ \underbrace{\ldots}_{t\,\text{бит}} \, .$$

Обозначим

$$e_1 = (\underbrace{0 \ldots 0}\ 1\ \underbrace{0 \ldots 0}_{t\,\text{бит}}); \quad e_m = (\underbrace{0 \ldots 0}\ 1\ \underbrace{0 \quad \ldots \quad 0}_{t+m+1\,\text{бит}}); \quad e_{tm} = e_t \oplus e_m \ .$$

Рассмотрим действие операции модульного сложения в группе $\mathbb{Z}_{2^n}$ на элементы фактор-группы группы $(V_n, \oplus)$ по выбранной подгруппе $H_{t,m}$ относительно операции побитового сложения.

Выпишем все классы смежности по этой подгруппе:

$$H_1 = H_{t,m}\ ; \qquad H_3 = e_m \oplus H_{t,m}\ ;$$
$$H_2 = e_t \oplus H_{t,m}\ ; \quad H_4 = e_{tm} \oplus H_{t,m}\ .$$

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

Таблица 3. Вероятности попадания суммы векторов v_1 и v_2 в соответствующий класс смежности H_i, $i = 1, \ldots, 4$ (для примера 1)

	$v_2 \in H_1$		$v_2 \in H_2$		$v_2 \in H_3$		$v_2 \in H_4$	
$v_1 \in H_1$	H_1 $p_t p_m$	H_2 $q_t p_m$	H_1 $q_t q_m$	H_2 $p_t p_m$	H_1 $p_t q_m$	H_2 $q_t q_m$	H_1 $q_t p_m$	H_2 $p_t q_m$
	H_3 $p_t q_m$	H_4 $q_t q_m$	H_3 $q_t p_m$	H_4 $p_t q_m$	H_3 $p_t p_m$	H_4 $q_t p_m$	H_3 $q_t q_m$	H_4 $p_t p_m$
$v_1 \in H_2$	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$	$p_t p_m$	$q_t p_m$
	$q_t p_m$	$p_t q_m$	$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$
$v_1 \in H_3$	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$	$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$
	$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$
$v_1 \in H_4$	$q_t p_m$	$p_t q_m$	$p_t p_m$	$q_t p_m$	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$
	$q_t q_m$	$p_t p_m$	$p_t q_m$	$q_t q_m$	$q_t p_m$	$p_t q_m$	$p_t p_m$	$q_t p_m$

Таблица 4. Вероятности попадания разности векторов v_1 и v_2 в соответствующий класс смежности H_i, $i = 1, \ldots, 4$ (для примера 1)

$v_1, v_2 \in H_i$	Вероятности попадания в H_i			
	H_1	H_2	H_3	H_4
H_i, $i = 1, \ldots, 4$	$p_t p_m$	$q_t q_m$	$p_t q_m$	$q_t p_m$

Пример 2. Пусть H_t — подгруппа $(V_n, \oplus)$, индекс которой равен четырем, а ее элементы имеют следующий вид:

$$\underbrace{\ldots}\ 0\ \underbrace{\ldots}_{t\text{ бит}}\ 0\,.$$

Выпишем все классы смежности по этой подгруппе:

$$H_1 = \underbrace{\ldots}\ 0\ \underbrace{\ldots}_{t\text{ бит}}\ 0\,; \qquad H_3 = \underbrace{\ldots}\ 1\ \underbrace{\ldots}\ 0\,;$$

$$H_2 = \underbrace{\ldots}\ 0\ \underbrace{\ldots}\ 1\,; \qquad H_4 = \underbrace{\ldots}\ 1\ \underbrace{\ldots}\ 1\,.$$

Рассмотрим действие операции модульного сложения в группе $\mathbb{Z}_{2^n}$ на элементы фактор-группы группы $(V_n, \oplus)$ 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 $i, j, k = 1, \ldots, 4$, описываются табл. 5, симметричной относительно главной диагонали, а вероятности $P(v_1 - v_2 \in H_i \,/\, v_1, v_2 \in H_j)$, где $i, j, k = 1, \ldots, 4$, описываются табл. 6.

Таблица 5. Вероятности попадания суммы векторов v_1 и v_2 в соответствующий класс смежности H_i, $i=1,\ldots,4$ (для примера 2)

	$v_2 \in H_1$		$v_2 \in H_2$		$v_2 \in H_3$		$v_2 \in H_4$	
$v_1 \in H_1$	H_1 p_t	H_2 0	H_1 0	H_2 p_t	H_1 q_t	H_2 0	H_1 0	H_2 q_t
	H_3 q_t	H_4 0	H_3 0	H_4 q_t	H_3 p_t	H_4 0	H_3 0	H_4 p_t
$v_1 \in H_2$	0	p_t	q_t	0	0	q_t	p_t	0
	0	q_t	p_t	0	0	p_t	q_t	0
$v_1 \in H_3$	q_t	0	0	q_t	p_t	0	0	p_t
	p_t	0	0	p_t	q_t	0	0	q_t
$v_1 \in H_4$	0	q_t	p_t	0	0	p_t	q_t	0
	0	p_t	q_t	0	0	q_t	p_t	0

Таблица 6. Вероятности попадания разности векторов v_1 и v_2 в соответствующий класс смежности H_i, $i=1, \ldots, 4$ (для примера 2)

$v_1, v_2 \in H_i$	Вероятности попадания в H_i			
	H_1	H_2	H_3	H_4
H_i, $i=1, \ldots, 4$	p_t	0	q_t	0

Следует отметить, что если в подгруппе имеются только нулевые блоки единичной длины, то количество классов смежности, в которые сумма векторов по модулю 2^n попадает с ненулевой вероятностью, будет наибольшим; если нулевые блоки будут большой длины, то количество классов смежности, в которые сумма векторов по модулю 2^n попадает с ненулевой вероятностью, уменьшается. Чем длиннее нулевые блоки, тем в меньшее количество классов смежности попадает сумма векторов по модулю 2^n с ненулевой вероятностью. Таким образом, перемешивающие свойства операции модульного сложения относительно побитового сложения будут зависеть от структуры подгруппы.

ВЛИЯНИЕ ОПЕРАЦИИ ПОБИТОВОГО СЛОЖЕНИЯ НА СТРУКТУРУ ФАКТОР-ГРУПП $(\mathbb{Z}_{2^n}, +)$ ПО ЕЕ ПОДГРУППЕ ИНДЕКСА 2^k ОТНОСИТЕЛЬНО МОДУЛЬНОГО СЛОЖЕНИЯ

Теорема 2. Пусть G_k — подгруппа $(\mathbb{Z}_{2^n}, +)$ индекса 2^k. Тогда:

1) G_k (в соответствующем представлении) — подгруппа $(V_n, \oplus)$;

2) классы смежности по подгруппе G_k (относительно операции $+$) имеют вид $i+G_k$, $0 \le i < 2^k$;

3) классы смежности по подгруппе G_k (относительно операции $\oplus$) имеют вид $i \oplus G_k$, причем $i \oplus G_k = i+G_k$, $0 \le i < 2^k$;

4) если $v_1, v_2 \in i+G_k$, то с вероятностью единица $v_1 \oplus v_2 \in G_k$, $0 \le i < 2^k$;

5) если $v_1, v_2 \in i \oplus G_k$, то с вероятностью единица $v_1 - v_2 \in G_k$, $0 \le i < 2^k$;

6) если $v_1 \in i+G_k$, $v_2 \in j+G_k$, то с вероятностью единица $v_1 \oplus v_2 \in i \oplus j+G_k$, причем класс смежности $i \oplus j+G_k$ может не совпадать с классом смежности $i+j+G_k$, $0 \le i, j < 2^k$;

7) если $v_1 \in i \oplus G_k$, $v_2 \in j \oplus G_k$, то с вероятностью единица $v_1 + v_2 \in i + j + G_k$, $0 \le i, j < 2^k$.

Доказательство. Не ограничивая общности, предположим, что подгруппа содержит один нулевой блок из двух битов. Для нулевого блока большей длины доказательство проводится аналогично. Выберем подгруппу G_2 группы $(V_n, \oplus)$, индекс которой равен 4, таким образом, что ее элементы имеют вид

$$\underbrace{\ldots}_{n-2\,\text{бит}}\,00\,.$$

Выпишем все классы смежности по этой подгруппе:

$$H_1 = \underbrace{\ldots}_{n-2\,\text{бит}}\,00\,; \qquad H_3 = \underbrace{\ldots}_{n-2\,\text{бит}}\,10\,;$$

$$H_2 = \underbrace{\ldots}_{n-2\,\text{бит}}\,01\,; \qquad H_4 = \underbrace{\ldots}_{n-2\,\text{бит}}\,11\,.$$

Рассмотрим действие операции модульного сложения в группе $\mathbb{Z}_{2^n}$ на элементы фактор-группы группы $(V_n, \oplus)$ по выбранной подгруппе G_2 относительно операции побитового сложения. Тогда вероятности $P(v_1 + v_2 \in H_i \,/\, v_1 \in H_j,\ v_2 \in H_k)$, где $i, j, k = 1, \ldots, 4$, описываются табл. 7, симметричной относительно главной диагонали, а вероятности $P(v_1 - v_2 \in H_i \,/\, v_1, v_2 \in H_j)$, где $i, j, k = 1, \ldots, 4$, описываются табл. 8.

Таблица 7. Вероятности попадания суммы векторов v_1 и v_2 по модулю 2^n в соответствующий класс смежности H_i, $i = 1, \ldots, 4$

	$v_2 \in H_1$		$v_2 \in H_2$		$v_2 \in H_3$		$v_2 \in H_4$	
$v_1 \in H_1$	H_1 1	H_2 0	H_1 0	H_2 1	H_1 0	H_2 0	H_1 0	H_2 0
	H_3 0	H_4 0	H_3 0	H_4 0	H_3 1	H_4 0	H_3 0	H_4 1
$v_1 \in H_2$	0	1	0	0	0	0	1	0
	0	0	1	0	0	1	0	0
$v_1 \in H_3$	0	0	0	0	1	0	0	1
	1	0	0	1	0	0	0	0
$v_1 \in H_4$	0	0	1	0	0	1	0	0
	0	1	0	0	0	0	1	0

Докажем сначала результаты табл. 7. Рассмотрим для примера доказательство некоторых возможных случаев, поскольку доказательство остальных случаев проводится аналогично.

1. Пусть $v_1, v_2 \in H_1$, тогда векторы v_1 и v_2 имеют следующий вид:

$$v_1 = \underbrace{\ldots}_{n-2\,\text{бит}}\,00\,; \qquad v_2 = \underbrace{\ldots}_{n-2\,\text{бит}}\,00\,.$$

Таблица 8. Вероятности попадания разности векторов v_1 и v_2 по модулю 2^n в соответствующий класс смежности H_i, $i=1,\ldots,4$

$v_1, v_2 \in H_i$	Вероятности попадания в H_i			
	H_1	H_2	H_3	H_4
H_i, $i=1,\ldots,4$	1	0	0	0

Очевидно, что сумма этих векторов по v_1 модулю 2^n всегда будет попадать в этот же класс смежности, а именно

$$P(v_1+v_2 \in H_1)=1; \quad P(v_1+v_2 \in H_3)=0;$$
$$P(v_1+v_2 \in H_2)=0; \quad P(v_1+v_2 \in H_4)=0.$$

2. Пусть $v_1 \in H_2$, а $v_2 \in H_4$. Тогда векторы v_1 и v_2 имеют следующий вид:

$$v_1 = \underbrace{\ldots}_{n-2\,\text{бит}}01; \qquad v_2 = \underbrace{\ldots}_{n-2\,\text{бит}}11.$$

Сумма этих векторов по модулю 2^n всегда будет попадать в класс смежности H_1, т.е.

$$P(v_1+v_2 \in H_1)=1; \quad P(v_1+v_2 \in H_3)=0;$$
$$P(v_1+v_2 \in H_2)=0; \quad P(v_1+v_2 \in H_4)=0.$$

Докажем теперь результаты табл. 8. Для примера рассмотрим случай, когда $v_1 \in H_3, v_2 \in H_3$. Тогда эти векторы имеют вид

$$v_1 = \underbrace{\ldots}_{n-2\,\text{бит}}10; \qquad v_2 = \underbrace{\ldots}_{n-2\,\text{бит}}10.$$

Разность данных векторов по модулю 2^n всегда будет попадать в класс смежности H_1, т.е.

$$P(v_1-v_2 \in H_1)=1; \quad P(v_1-v_2 \in H_3)=0;$$
$$P(v_1-v_2 \in H_2)=0; \quad P(v_1-v_2 \in H_4)=0.$$

Рассмотрим действие операции побитового сложения в группе V_n на элементы фактор-группы группы $(\mathbb{Z}_{2^n}, +)$ по выбранной подгруппе G_2 относительно операции модульного сложения. Следует отметить, что классы смежности по подгруппе G_2 относительно модульного сложения будут в точности совпадать с выписанными выше классами смежности H_1, H_2, H_3, H_4 относительно операции побитового сложения. Тогда вероятности $P(v_1 \oplus v_2 \in H_i / v_1 \in H_j, v_2 \in H_k)$, где $i, j, k = 1,\ldots,4$, описываются табл. 9, симметричной относительно главной диагонали, а вероятности $P(v_1 - v_2 \in H_i / v_1, v_2 \in H_j)$, где $i, j, k = 1,\ldots,4$, описываются табл. 10.

Докажем результаты табл. 9. Рассмотрим доказательство некоторых возможных случаев.

1. Пусть $v_1, v_2 \in H_1$, тогда векторы v_1 и v_2 имеют следующий вид:

$$v_1 = \underbrace{\ldots}_{n-2\,\text{бит}}00; \qquad v_2 = \underbrace{\ldots}_{n-2\,\text{бит}}00.$$

Таблица 9. Вероятности попадания побитовой суммы векторов v_1 и v_2 в соответствующий класс смежности H_i, $i=1,\ldots,4$

	$v_2 \in H_1$		$v_2 \in H_2$		$v_2 \in H_3$		$v_2 \in H_4$	
$v_1 \in H_1$	H_1 1	H_2 0	H_1 0	H_2 1	H_1 0	H_2 0	H_1 0	H_2 0
	H_3 0	H_4 0	H_3 0	H_4 0	H_3 1	H_4 0	H_3 0	H_4 1
$v_1 \in H_2$	0	1	1	0	0	0	0	0
	0	0	0	0	0	1	1	0
$v_1 \in H_3$	0	0	0	0	1	0	0	1
	1	0	0	1	0	0	0	0
$v_1 \in H_4$	0	0	0	0	0	1	1	0
	0	1	1	0	0	0	0	0

Таблица 10. Вероятности попадания побитовой разности векторов v_1 и v_2 в соответствующий класс смежности H_i, $i=1, \ldots, 4$

$v_1, v_2 \in H_i$	Вероятности попадания в H_i			
	H_1	H_2	H_3	H_4
H_i, $i=1, \ldots, 4$	1	0	0	0

Очевидно, что побитовая сумма этих векторов всегда будет попадать в этот же класс смежности, т.е.

$$P(v_1 \oplus v_2 \in H_1)=1; \quad P(v_1 \oplus v_2 \in H_3)=0;$$

$$P(v_1 \oplus v_2 \in H_2)=0; \quad P(v_1 \oplus v_2 \in H_4)=0.$$

2. Пусть $v_1 \in H_2$, $v_2 \in H_4$. Тогда векторы v_1 и v_2 имеют следующий вид:

$$v_1 = \underbrace{\ldots}_{n-2\,\text{бит}} 01; \qquad v_2 = \underbrace{\ldots}_{n-2\,\text{бит}} 11.$$

Побитовая сумма этих векторов в отличие от операции сложения по модулю 2^n всегда будет попадать в класс смежности H_3, т.е.

$$P(v_1 \oplus v_2 \in H_1)=0; \quad P(v_1 \oplus v_2 \in H_3)=1;$$

$$P(v_1 \oplus v_2 \in H_2)=0; \quad P(v_1 \oplus v_2 \in H_4)=0.$$

Докажем результаты табл. 10. Для примера рассмотрим следующий случай, когда $v_1 \in H_3$, $v_2 \in H_3$. Тогда эти векторы имеют вид

$$v_1 = \underbrace{\ldots}_{n-2\,\text{бит}} 10; \qquad v_2 = \underbrace{\ldots}_{n-2\,\text{бит}} 10.$$

Побитовая разность данных векторов, так же как и разность по модулю 2^n, всегда попадает в класс смежности H_1, т.е.

$$P(v_1 - v_2 \in H_1)=1; \quad P(v_1 - v_2 \in H_3)=0;$$

$$P(v_1 - v_2 \in H_2)=0; \quad P(v_1 - v_2 \in H_4)=0.$$

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

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

то операция побитового (модульного) сложения сохраняет структуру соответствующей фактор-группы относительно модульного (побитового) сложения.

ЗАКЛЮЧЕНИЕ

Результаты, полученные в данной статье, характеризуют перемешивающие свойства операций побитового и модульного сложения, заданных на одном носителе. Наиболее интересным является тот факт, что действие операции модульного сложения на фактор-группу относительно операции побитового сложения существенно зависит от выбора подгруппы в $(V_n, \oplus)$, а операция побитового сложения всегда сохраняет структуру соответствующей фактор-группы по любой подгруппе в $(\mathbb{Z}_{2^n}, +)$.

Данные результаты показывают потенциальную возможность применения атаки гомоморфизмов (групповой атаки) при некоторых дополнительных условиях в том случае, когда в раундовых функциях блочного шифра используются разные операции, например в шифрах «Калина», «Мухомор» и некоторых других.

СПИСОК ЛИТЕРАТУРЫ

1. Шемякина О.В. О перемешивающих свойствах операций в конечном поле // Тр. Восьмой Общерос. науч. конф. «Математика и безопасность информационных технологий» (МаБИТ-09), 30 окт. — 2 нояб. 2009. — М.: МЦНМО, 2010. — **2**. — С. 87–90.
2. Горчинский Ю.Н. О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями // Тр. по дискрет. математике. — М.: ТВП, 1997. — **1**. — С. 67–84.
3. Горчинский Ю.Н. Стохастические алгебры // Там же. — **2**. — С. 55–87.
4. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. — М.: Госстандарт СССР, 1989. — 28 с.
5. Горбенко И.Д., Тоцький О.С., Казьміна С.В. Перспективний блоковий шифр «Калина» — основні положення та специфікація // Приклад. радіоелектроніка. — 2007. — **6**, № 2. — С. 195–208.
6. Lai X., Massey J.L., Murphy S. Markov ciphers and differential cryptanalysis // Adv. in Cryptology — EUROCRYPT'91: Proc. — Berlin: Springer-Verlag, 1991. — P. 17–38.
7. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. — 1991. — **4**, N 1. — P. 3–72.
8. Berson T.A. Differential cryptanalysis mod 232 with applications to MD5 // Adv. in Cryptology. — CRYPTO'98 (LNCS 372): Proc. — New York: Springer-Verlag, Inc., 1999. — P. 95–103.
9. Ковальчук Л.В. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига // Кибернетика и системный анализ. — 2010. — № 6. — С. 89–96.

Поступила 19.01.2011