Н.В.ПАЦЕЙ, П.П.УРБАНОВИЧ

Белорусский государственный технологический университет
(г.Минск)

ОБЩИЕ ДИФФУЗИОННЫЕ ХАРАКТЕРИСТИКИ КРИПТОГРАФИЧЕСКИХ БЛОЧНЫХ КОДОВ

При разработке алгоритмов криптографических преобразований, дополненных корректирующими кодами, возникает вопрос: насколько эффективным будет совместное использование помехоустойчивых кодов и криптопреобразований? Наиболее достоверный ответ на этот вопрос можно получить только на основе изучения реальных статистических данных об общих диффузионных характеристиках блочных шифров. В данном случае под диффузией данных понимается преобразование каждого входного байта информации в каждый выходной путем перемешивания, а именно путем полной произвольной подстановки (overall random substitution). Диффузионные свойства относительно просто проверяются следующим экспериментом. Для некоторого ключа выбираем случайный блок данных и шифруем исходный текст. Затем изменяем один бит в шифротексте (1→0 или 0→1), дешифрируем его и сравниваем результат с первоначальным открытым текстом, подсчитывая число искаженных бит в тексте. Повторяем эту процедуру для различных симметричных блочных алгоритмов, например, MMB, 3–Way, IDEA, FEAL8, RC5 и Blowfish. В частности, на рис. 1 приведены гистограммы для двух алгоритмов 3–Way и IDEA со следующими параметрами:

Алгоритм	Размер блока, бит	Размер ключа, бит
3-Way	96	96
IDEA	64	128

В процессе обработки экспериментальных результатов установлено, что даже сравнительно большое число экспериментов (1234 с 3–Way и 800 с IDEA алгоритмом, что является достаточным для перехода от понятия относительной частоты к вероятности) дает очень ограниченный диапазон искаженных бит в блоке, который не превышает 10% размера блока. Условия проведенных независимых экспериментов с алгоритмами описываются *схемой Бернулли* [1], что указывает на биномиальное распределение вероятности. Тогда формула вероятности нахождения любого определенного числа изменений c бит в b битном блоке будет иметь следующий стандартный вид:

$$P(c) = \frac{\binom{b}{c}}{2^b} = \frac{b!\,2^b}{(b-c)!\,c!} \qquad (1)$$

Огибающая линия на гистограммах построена на основе теоретических данных, рассчитанных по формуле (1). Из гистограмм видно, что полученные статистические результаты с небольшой погрешностью соответствуют биномиальному распределению вероятности.

Как показали результаты исследований, при дешифрировании шифротекстов со случайным искажением бита информации приблизительно от одной до двух третей открытого текста оказывается искаженным. Фактически это означает потерю блока информации и является решающим аргументом в пользу добавления процедур коррекции ошибок к криптоалгоритмам.

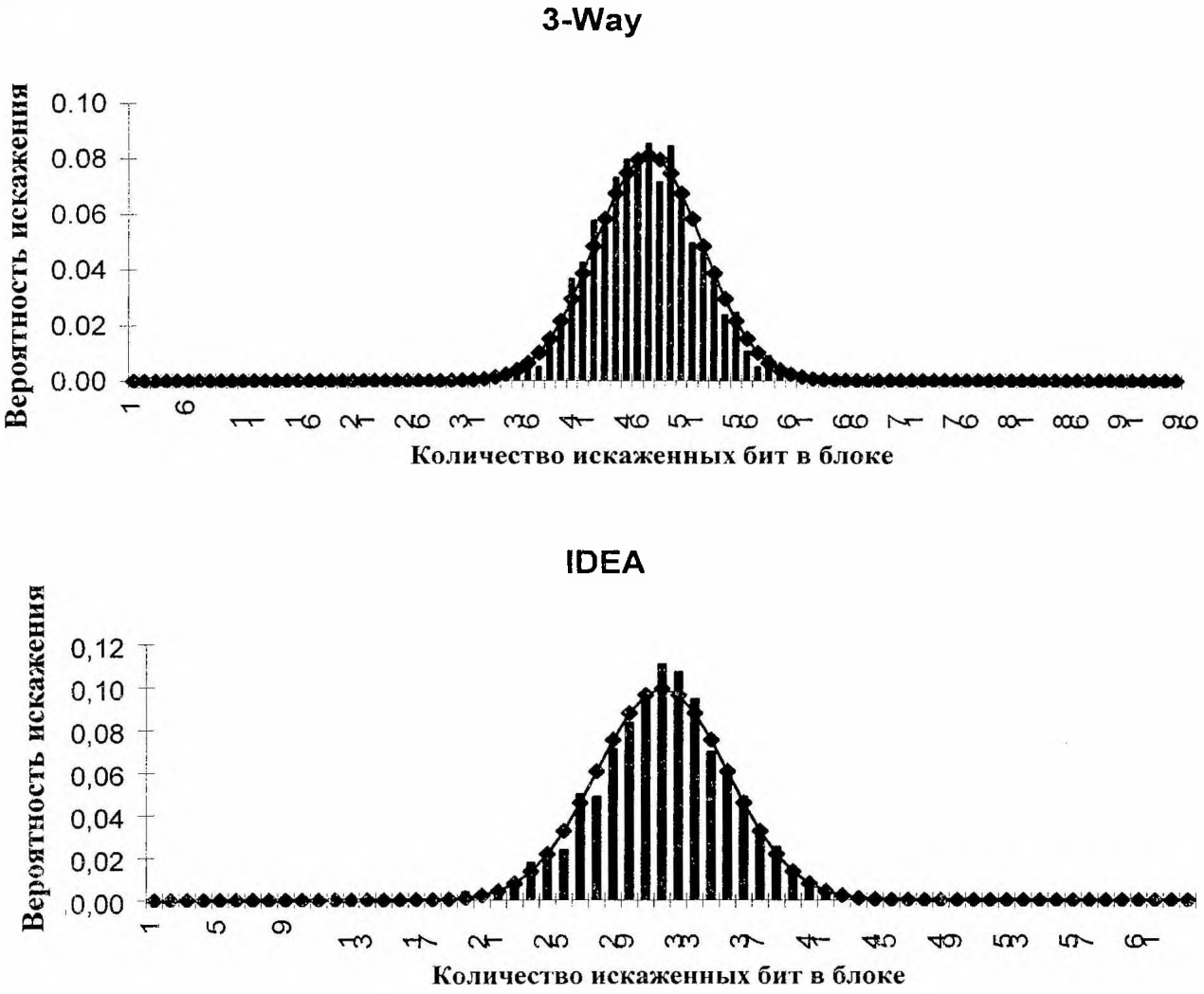

Рис. 1. Гистограммы зависимости количества искаженных бит в блоке при введении единичной ошибки в шифротекст; экспериментальные (столбцы) и теоретические (линия с точками) данные

Литература

1. Герасимович А. И. Математическая статистика. -Мн., 1983.
2. B. Schneier. Description of a new variable-lenght key, 64–bit block cipher (Blowfish), Fast Software Encryption, Lecture Notes in Computer Science, Vol. 809, Springer-Verlag, 1994, pp. 359–362.
3. Cryptographic Algorithms URL: http://www.mach5.com/crypto/algorithms.html