0.1. *Пестунов А.И., Перов А.А.* **Анализ статистических свойств легковесных блочных шифров с помощью специализированной программной библиотеки**

Генерация псевдослучайных чисел — это одно из распространённых применений итеративных блочных шифров, причём удовлетворительные статистические свойства выходной последовательности могут быть обеспечены значительно меньшим числом раундов (R_{min}), чем полное число раундов шифра (R), призванное обеспечить криптографическую стойкость. Для экспериментальной оценки R_{min} необходимо провести анализ статистических свойств генерируемой шифром последовательности при возрастающем числе раундов, улучшая статистические свойства. Начиная с некоторого числа раундов, генерируемая последовательность перестанет отличаться от случайной (с помощью используемого критерия), и это число раундов можно принять в качестве оценки R_{min}.

Для проведения анализа целесообразно использовать программные коды шифров, имеющиеся в открытом доступе, однако их интеграция в собственные программы во многом затруднена из-за различных сигнатур функций шифрования и развертывания ключа у разных реализаций. Две наиболее существенные проблемы, затрудняющие автоматизированную обработку шифров, следующие: во-первых, число раундов не выносится в качестве аргумента функции и, во-вторых, блоки представляются в виде слов разной длины (например, 128-битовый блок может быть представлен как четыре 32-битовых слова или как шестнадцать 8-битовых). В настоящей статье представлена созданная на базе открытых исходных кодов шифров программная библиотека, предоставляющая единый интерфейс для обращения к шифрам и приводятся результаты статистического анализа малоресурсных алгоритмов с её помощью (см. табл. 1). Значительная часть реализаций шифров взята из библиотеки BLOC [1]. Для статистического анализа использован тест “стопка книг” [2].

Работа поддержана грантом РФФИ, проект № 14-01-31484 (мол_а).

Таблица 1: Оценка минимального числа раундов (R_{min}), обеспечивающее удовлетворительные статистические свойства шифров; R — полное число.

Шифр	R_{min}	R	Шифр	R_{min}	R
XTEA	3	32	Piccolo	6	25–31
SPECK	6	22–34	KLEIN	4	12–20
CLEFIA	6	18–26	mCrypton	6	12
LED	4	32–48	Noekeon	2	16
MIBS	2	32	IDEA	2	8.5
AES	4	10–14	DESXL	2	8
Lblock	9	32	Present	9	31
Twine	9	36	Hight	10	32
Sea	10	51	Skipjack	14	32
Simon	18	32–72	Katan64, Ktantan64	30	254

Список литературы

[1] Cazorla M., Marquet K., Minier M. Survey and benchmark of lightweight block ciphers for wireless sensor networks // Proc. 10th International Conference on Security and Cryptography (SECRYPT-2013). — Pp. 543–548.

[2] Рябко Б. Я., Пестунов А. И. “Стопка книг” как новый статистический тест для случайных чисел // Проблемы передачи информации. — 2004. — Т. 40, № 1. С. 73–78.