2. Facialmapping (landmarks) withDlib + python. [Электронныйресурс]. Режим доступа:https://towardsdatascience.com/facial-mapping-landmarks-with-dlib-python. Дата доступа: 06.04.2023.

3. OpenCV [Электронный ресурс]. Режим доступа: https://blog. skillfactory.ru /glossary/opencv/. Датадоступа: 05.04.2023.

4. Системы распознавания лиц. [Электронный ресурс]. Режим доступа:https://www.tadviser.ru/index.php/Facial_recognition. Дата доступа: 10.04.2023.

УДК 004.056.5:004.021

Студ. А.В. Почебут, В.В. Максимова
Науч. рук. проф. П.П. Урбанович
(Кафедра информационных систем и технологий, БГТУ)

СРАВНИТЕЛЬНАЯ ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ И КРИПТОСТОЙКОСТИ АЛГОРИТМОВ RC4 И RC4+

Алгоритмы RC4 и RC4+ играют важную роль в повышении защищенности информации [1]. Ключевая разница между RC4 и RC4+ в дополнительном блоке EKSA, который повышает криптографическую стойкость алгоритма. RC4 состоит из двух блоков: KSA (Key-Scheduling Algorithm), производящего обработку ключа для генерации псевдослучайной последовательности ключей (до 256 бит), а также PRGA (Pseudo-Random Generation Algorithm), выполняющего генерацию псевдослучайной последовательности ключей. В RC4+ EKSA (Extended Key-Scheduling Algorithm) блок идет следом за KSA блоком [1–3].

EKSA – это дополнительный блок в алгоритме KSA в RC4+, который улучшает безопасность шифра путем добавления дополнительных итераций в KSA, используя два ключа длиной 128 битов каждый. Этот блок делает дополнительные шаги обработки ключа перед генерацией ключевого потока, которые включают в себя дополнительные перестановку в KSA блоке и добавление к ключу дополнительного блока битов. Это повышает стойкость алгоритма и уменьшает вероятность успешной атаки на систему шифрования. При использовании коротких ключей (например, менее 128 бит) применение EKSA может привести к увеличению количества обращений к комбинации, содержащей оригинальный ключ, необходимой для генерации псевдослучайной последовательности ключей, что в свою очередь может повысить вероятность обнаружения ключевого потока и ухудшить стойкость алгоритма. Однако, при использовании достаточно длинных ключей, применение EKSA может повысить криптостойкость алгоритма RC4+.

Вычислительная сложность (ComputationalComplexity), *O*, оценивается путем выяснения общего количества операций, произведенных как вKSA, так и в PRGA. Чем больше количество операций, тем выше будет сложность шифра. Сложность каждого варианта анализируется следующим образом: в базовом RC4 в KSA кол-во операцийN_1= 3 · 256 = 768, где 256 – общее количество битов в выходном наборе данных из KSA блока, и в PRGA: N_2= =6·*N* = 6*N*. Здесь *N*– количество байтов открытого текста. Например, если *N*= = 40, то количество итераций в PRGA будет 40, а количество операций будет 240. Таким образом, вычислительная сложность RC4: CC = 768 + 6N (общее количество операций в KSA + PRGA), а вычислительная сложность RC4+: *O*=4608 + 16*N*.

В таблице представлены количественные результаты выполненного сравнения алгоритмов.

Таблица – Вычислительная сложность алгоритмов

Реализации RC4	Алгоритм	Типы операций					Суммарное количество операций	*O*
		XOR	SWAP	ADD	MOD	SHIFT		
RC4	KSA	0	1	1	1	0	3·256 = 768	768+6*N*
	PRGA	1	1	2	2	0	6*N*	
RC4+	KSA+	2	4	6	6	0	18 ·256 = 4608	4608+16*N*
	PRGA+	4	1	4	3	4	16*N*	

Подводя итог, отметим, что сравнение проведенных результатов практических испытаний с теоретическими данными относительно вычислительной сложности алгоритмов близки.

Также необходимо упомянуть, что, несмотря на то, что RC4+ более чем в два раза затратнее, чем RC4, его криптостойкость (оцениваем по сложности вычисления) в 6 раз выше.

ЛИТЕРАТУРА

1. Урбанович, П. П. Лабораторный практикум по дисциплинам «Защита информации и надежность информационных систем» и «Криптографические методы защиты информации». В 2 ч. Ч. 2. Криптографические и стеганографические методы защиты информации: учеб.-метод. пособие для студ. вузов / П. П. Урбанович, Н. П. Шутько. – Минск: БГТУ, 2020. – 226 с.

2. Measuring Avalanche Properties on RC4 Stream Cipher Variants / E. J Madarro-Capó [at. Al.], Appl. Sci. 2021, 11(20), 9646; https://doi.org/10.3390/app11209646/

3. Progress in Cryptology – INDOCRYPT 2013: 14th International Conference on Cryptology in India, Mumbai, India, December 7-10, 2013.