УДК 004.056.55

К. В. Филимонов, А. И. Тур
Пермский национальный исследовательский
политехнический университет, г. Пермь

АНАЛИЗ ЭФФЕКТИВНОСТИ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА CHACHA ДЛЯ ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ДАННЫХ ДЛЯ МИКРОКОНТРОЛЛЕРА ESP8266

В данной работе рассмотрен алгоритм симметричного шифрования ChaCha и его реализация в стандартных библиотеках. Произведен анализ эффективности криптографического алгоритма при различном числе итераций.

Ключевые слова: IOT, ChaCha, esp8266, шифрование, эффективность, микроконтроллеры.

K. V. Filimonov, A. I. Tur
Perm national research polytechnic university, Perm

ANALYSIS OF THE EFFICIENCY OF THE CHACHA CRYPTOGRAPHIC ALGORITHM FOR SECURE DATA TRANSMISSION FOR ESP8266 MICROCONTROLLER

In this paper, the ChaCha symmetric encryption algorithm and its implementation in standard libraries are considered. The analysis of the effectiveness of the cryptographic algorithm for a different number of iterations was carried out.

Keywords: IOT, ChaCha, esp8266, encryption, effectiveness, microcontrollers.

Развитие технологий Интернета Вещей, Internet of things, ведет к существенному увеличению числа устройств, подключенных к сети интернет.

При передаче данных по открытым каналам связи возникает угроза перехвата трафика. Для обеспечения защиты информации необходимо шифрование пакетов. Однако в связи с ограниченными вычислительными ресурсами, операции шифрования и дешифрования могут оказаться крайне неэффективными. В связи с этим возникает проблема выбора наиболее эффективного алгоритма шифрования, который обладал бы одновременно достаточной криптостойкостью для противодействия активным атакам и относительно быстрым временем проведения криптографических операций.

В этой работе мы не будем рассматривать криптоанализ и криптографические атаки.

Алгоритм ChaCha рекомендуется разработчиками официальной криптографической библиотеки. Они считают, что ChaCha в два раза быстрее алгоритма AES128 и гораздо безопаснее. Последний же используется в случаях, когда необходима обратная совместимость со старыми протоколами.

ChaCha - симметричный поточный шифр, является модификацией

алгоритма Salsa. Оба используют псевдослучайный генератор чисел, основанный на технике add-rotate-XOR (ARX), использующий простейшие операции сложения по модулю 32, сдвигов, и сложения по модулю 2. Эта особенность позволяет добиться высокой эффективности при ограниченных вычислительных мощностях. Ключ шифрования и дешифрования одинаков для двух операций. Скоростью шифрования и криптостойкостью можно управлять путем оптимального выбора битности ключа, а также числа раундов. Раунд - один цикл битовых преобразований. Основными длинами ключа являются 128 и 256 бит.

В стандартной библиотеке реализован алгоритм ChaCha для 128 и 256 бит ключа для 8, 12, 20 раундов. Произведем тестирование алгоритма с различными параметрами. Ключ и вектор инициализации сгенерированы заранее:

```
Performance Tests:
ChaCha20 256-bit SetKey ... 4.49us per operation, 222667.56 per second
ChaCha20 256-bit Encrypt ... 0.62us per byte, 1610103.40 bytes per second
ChaCha20 256-bit Decrypt ... 0.62us per byte, 1607434.38 bytes per second
ChaCha20 128-bit SetKey ... 8.86us per operation, 112905.05 per second
ChaCha20 128-bit Encrypt ... 0.62us per byte, 1612293.74 bytes per second
ChaCha20 128-bit Decrypt ... 0.62us per byte, 1607999.80 bytes per second
ChaCha12 256-bit SetKey ... 4.43us per operation, 225988.70 per second
ChaCha12 256-bit Encrypt ... 0.48us per byte, 2071599.66 bytes per second
ChaCha12 256-bit Decrypt ... 0.48us per byte, 2064449.53 bytes per second
ChaCha12 128-bit SetKey ... 8.85us per operation, 112981.58 per second
ChaCha12 128-bit Encrypt ... 0.48us per byte, 2071599.66 bytes per second
ChaCha12 128-bit Decrypt ... 0.48us per byte, 2064516.13 bytes per second
ChaCha8 256-bit SetKey ... 4.43us per operation, 225988.70 per second
ChaCha8 256-bit Encrypt ... 0.41us per byte, 2415641.28 bytes per second
ChaCha8 256-bit Decrypt ... 0.42us per byte, 2405924.59 bytes per second
ChaCha8 128-bit SetKey ... 8.85us per operation, 112981.58 per second
ChaCha8 128-bit Encrypt ... 0.41us per byte, 2415550.10 bytes per second
ChaCha8 128-bit Decrypt ... 0.42us per byte, 2406015.04 bytes per second
```

Рисунок 1 – Вывод результатов операций шифрования через Serial интерфейс

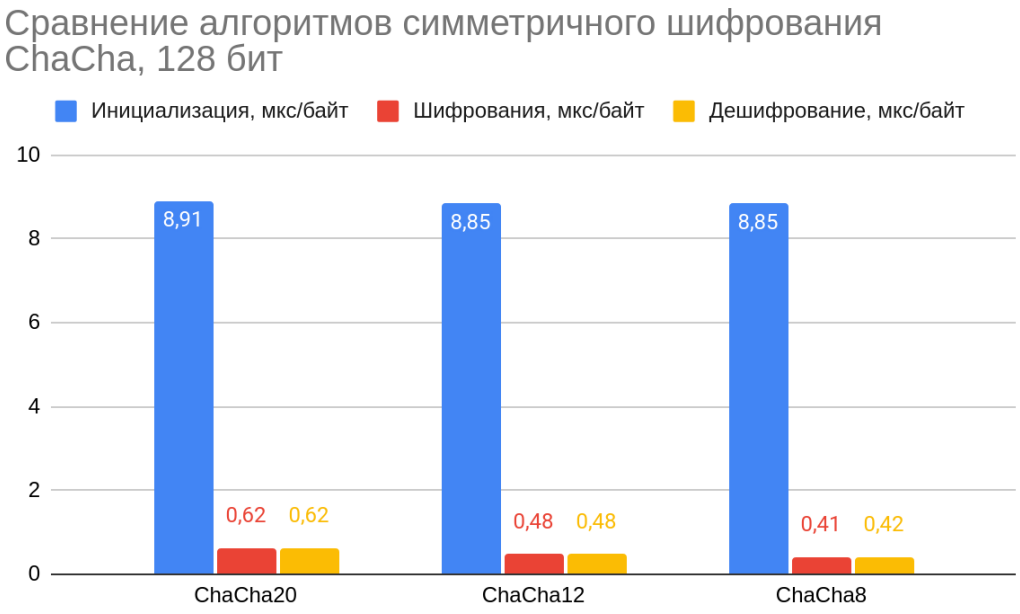

Рисунок 2 – Сравнение времени работы стадий ChaCha 128 бит с различным числом раундов

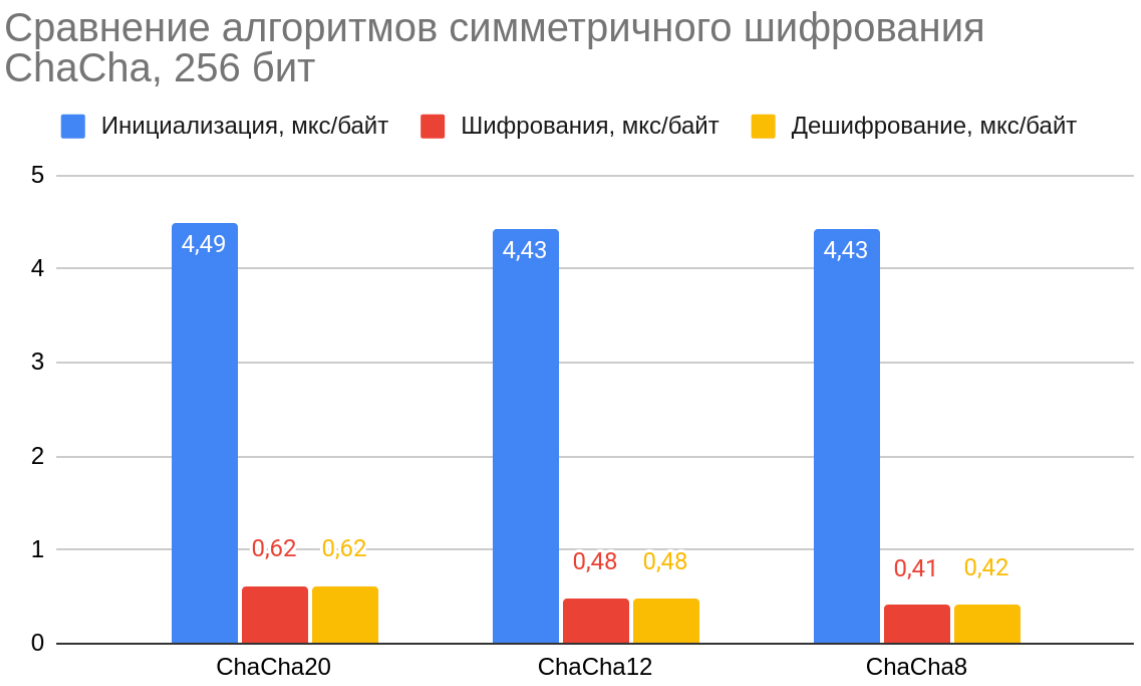

Рисунок 3 – Сравнение времени работы стадий ChaCha 256 бит с различным числом раундов.

Из полученных данных видно, что инициализация ключа занимает основную часть времени. Это связано с встроенными функциями работы с памятью. Для 128 бит вводится дополнительная функция, в этом можно убедиться при просмотре исходного кода функции инициализации памяти. Это может быть связано с защитой от криптографических атак.

Процедуры шифрования и дешифрования выполняются относительно быстро и не зависят от длины ключа. Разница во времени между 12 и 20 раундами достигает 50%. Это критично для задач с большим числом операций шифрования.

В целом стандарт в 20 раундов используется в большинстве современных приложений и его можно считать эффективным.

Список литературы

1.Nicolas Sklavos, I. D. Zaharakis (2016). Cryptography and Security in Internet of Things (IoT): Models, Schemes, and Implementations. DOI: 10.1109/NTMS.2016.7792443

2.Adri´an Ranea, Yunwen Liu, Tomer Ashur (2017). An Easy-To-Use Tool for Rotational-XOR Cryptanalysis of ARX Block Ciphers.

3.Arduino Cryptography Library - URL: https://rweather.github.io/arduinolibs/crypto.html

Сведения об авторах

Тур Александр Игоревич – ассистент кафедры «Автоматикаи телемеханика», Пермский национальный исследовательский политехнический университет, г. Пермь, email: tur.aleksandr93@mail.ru

Кирилл Вадимович Филимонов – студент Пермского национального исследовательского политехнического университета, гр. КЗИ-17-1б, г. Пермь, email: filimonov_kirill@protonmail.com

About the authors

Tur Aleksandr Igorevec – assistant of Department of Automation and remote control, Perm National Research Polytechnic University, Perm, email: tur.aleksandr93@mail.ru

Kirill Vadimovic Filimonov – Student of Perm National Research Polytechnic University, Perm, email: filimonov_kirill@protonmail.com