КОДЕК КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА БАЗЕ *RASPBERRY PI*

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Филиппов Н.С.

Саломатин С.Б. – к.т.н.,доцент

В работе рассмотрен и реализован алгоритм цифровой подписи, основанный на эллиптических кирвых, с целью использования в устройствах с ограниченной памятью. Произведено сравнение размеров ключей и криптостойкости по сравнению с наиболее популярным алгоритмом - *RSA.*

Обычные криптографические алгоритмы используются в системах с большими ресурсами, такими как сервера или персональные компьютеры. Встраиваемые системы, такие как: мобильные телефоны, смарт-карты, *RFID*-системы и т. д., обладают ограниченными ресурсами и требуют применения менее затратных алгоритмов.

В ходе работы был реализован алгоритм цифровой подписи *ECDSA* [1] (*Elliptic Curve Digital Signature Algorithm*) на языке программирования *Python* на устройстве *raspberry pi* [2] (рисунок 1). Данное устройство обладает следующими техническими характеристиками:

- Однокристалльная система SoC Broadcom BCM2835;
- Процессор 32-битный 1-ядерный ARMv6Z ARM1176JZF-S с тактовой частотой 1 ГГц;
- Графический 2-ядерный сопроцессор Video Core IV Multimedia;
- ОЗУ 512 Мб LPDDR2 SDRAM.
- WIFI 802.11n + Bluetooth 4.1 Low Energy (BLE).

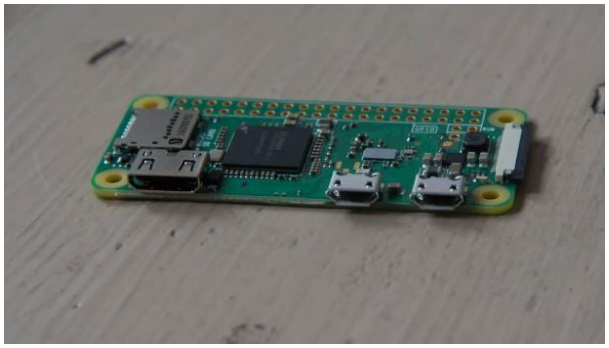

Рисунок 1 – *Raspberry pi zero w*

Для проведения эксперимета были взяты стандартизированные *NIST* (Национальный институт стандартов и технологий США) эллиптические кривые [3]: *Secp192k1, Secp192r1, Secp224r1, Secp256k1, Secp256r1, Secp384r1.*

NIST рекомендует формулу (1) для вычисления криптостойкости алгоритма *RSA* по длине ключа:

$$x = \frac{1.923 \cdot \sqrt[3]{L \cdot \ln(2)} \cdot \sqrt[3]{[\ln(L \cdot \ln(2))]^2} - 4.69}{\ln(2)}, \quad (1)$$

где *x* – уровень криптостойкость;
L – длина ключа.

Для вычисления криптостойкости *ECDSA* используется формула (2).

$$\mathrm{x} = \frac{L}{2}, \quad (2)$$

где *x* – уровень криптостойкость;
L – длина ключа.

Результаты сравнения размеров ключей *RSA* и *ECDSA* при заданном уровне криптостойкости приведены на рисунке 2.

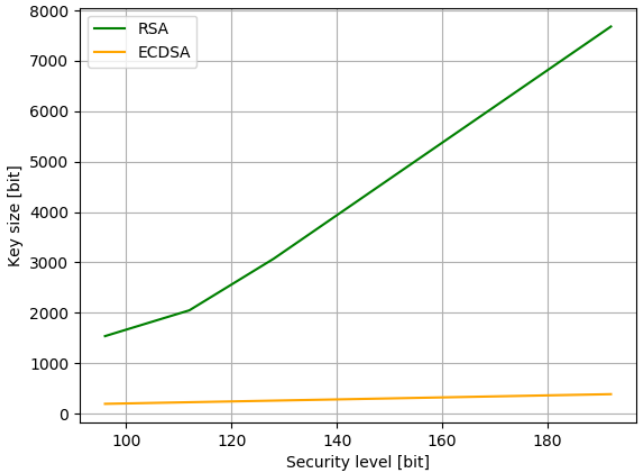

Рисунок 2 – График зависимости размера ключей *RSA* и *ECDSA* от уровня криптостойкости

График зависимости времени работы алгоритма от размера ключа представлен на рисунке 3.

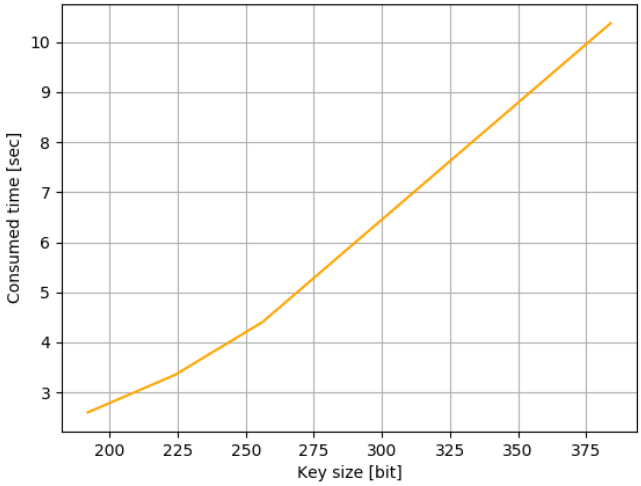

Рисунок 3 – График зависимости времени работы ECDSA от размера ключа

Для увеличения скорости работы данный алгоритм был реализован в виде веб-сервиса и размещен на облачном сервере, что позволило освободить устройство от большинства вычислений и увеличить скорость работы более, чем на порядок, а также использовать данный алгоритм в веб-приложениях.

В заключении, можно отметить, что *ECDSA* удовлетворяет условию ограниченной памяти, так как требуют гораздо меньше памяти для хранения секретного ключа, чем *RSA*. На данный момент был взломан ключ длиной 114 бит (23 августа 2017 года). Для этого потребовалось 2000 процессорных ядер и 6 месяцов вычислений, что подтверждает высокую криптостойкость данной системы.

Список использованных источников:

1. SEC 2: Recommended Elliptic Curve Domain Parameters. Daniel R. L. Brown. – NIST, 2010 – 37 с.
2. https://www.raspberrypi.org/products/raspberry-pi-zero-w/
3. Elliptic Curve Digital Signature Algorithm. D. Johnson, A. Meneses. – 2000 – 55 с.