УДК 004.056.55:629.735 **DOI: 10.31673/2412-9070.2023.034050**

О. І. БАРАННІК, аспірант,
Державний університет інформаційно-комунікаційних технологій, Київ

ПРОБЛЕМИ AES-ШИФРУВАННЯ БЕЗ АПАРАТНОГО ПРИСКОРЕННЯ НА ЧІПАХ BROADCOM BCM2711

У сучасному світі інформаційна безпека відіграє критичну роль у різних аспектах нашого життя. За останні десятиліття шифрування даних стало основним засобом забезпечення конфіденційності, цілісності та доступності інформації. Використовуючи сучасні алгоритми шифрування, можна захистити дані від несанкціонованого доступу та зловмисного використання.

З розвитком технологій одноплатові комп'ютери стають все більш популярними та функціональними. Використання одноплатових комп'ютерів може значно збільшити функціональність безпілотних літальних апаратів (БПЛА). Наприклад, використання одноплатового комп'ютера з можливістю оброблення відео в реальному часі може дати змогу БПЛА виконувати такі завдання, як моніторинг територій, відстеження об'єктів або навіть виконання пошуково-рятувальних операцій.

Однак пристрої, зокрема БПЛА, які потребують високої швидкості оброблення даних та низького енергоспоживання, часто обмежені відсутністю апаратного прискорення для алгоритмів шифрування, таких як AES [1]. Це призводить до стрімкого зниження швидкості шифрування та дешифрування. Таке обмеження вимагає від нас пошуку ефективних альтернатив алгоритму AES для зазначених пристроїв.

З огляду на ці обмеження та потребу в пошуках альтернатив метою цієї статті є порівняння роботи різних алгоритмів шифрування на процесорі Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit SoC [2]. Проаналізовано швидкість шифрування та дешифрування для алгоритмів AES-256, AES-512, ChaCha12 та ChaCha20, що дасть змогу зрозуміти, який алгоритм найефективніший для використання у системах керування БПЛА та інших пристроях, побудованих на Bcm2711, котрі не мають апаратного прискорення AES.

Ключові слова: шифрування; дешифрування; БПЛА; Raspberry Pi 4; AES; ChaCha20; апаратне прискорення; ChaCha12; алгоритмічна ефективність; одноплатові комп'ютери; безпроводові комунікації.

ВСТУП

Шифрування — процес перетворення інформації в новий формат, який є незрозумілим для тих, хто не має спеціального ключа, потрібного для дешифрування або перетворення інформації назад в її оригінальний формат. Це було вигадано тисячі років тому для забезпечення конфіденційності повідомлень між різними сторонами. Перші форми шифрування були простими й охоплювали методи, які змінювали порядок символів або замінювали їх іншими символами.

Види шифрування:

• *симетричне шифрування:* один ключ, який використовується і для шифрування, і для дешифрування. Прикладами симетричних алгоритмів шифрування можуть бути DES, AES, і Blowfish [3]. Це шифрування широко застосовується для шифрування даних, які перебувають у зберіганні, наприклад файлів на диску;

• *асиметричне шифрування:* для шифрування та дешифрування використовуються різні ключі. Зазвичай один ключ є публічним і може бути відкрито поширеним, а другий є приватним і має залишатися в таємниці. Приклади асиметричних алгоритмів шифрування такі: RSA, DSA, і ECC. Це часто використовується для обміну ключами та автентифікації;

• *хеш-функції:* це спеціальний тип шифрування, який перетворює дані у фіксовану довжину рядка символів, яка має випадковий вигляд. Хеш-функції широко використовуються для перевірки цілісності даних та зберігання паролів.

Важливість шифрування. Шифрування є критично важливим для захисту даних та конфіденційності інформації в цифровому світі. З його допомогою ми можемо захистити наші дані від несанкціонованого доступу та використання, а також забезпечити конфіденційність листування й особистої інформації. Без шифрування всі наші дані будуть відкриті для перегляду та використання зловмисниками.

Випадки викрадення інформації. Історія повна прикладів витоку нешифрованих даних, які призводили до серйозних наслідків. Наприклад, у 2017 році було виявлено, що компанія «Equifax», одна з найбільших кредитних бюро в США, стала жертвою витоку даних [4], який стосувався понад 143 млн американців. Зловмисники отримали доступ до імен, номерів соціального страхування, дат народження, адрес та іншої інформації, яку не було належним чином захищено. Це призвело до масової крадіжки ідентичності та фінансових збитків для багатьох людей.

Інший випадок відбувся 2018 року, коли компанія «Facebook» була змушена визнати, що дані 87 млн

їхніх користувачів були неправильно передані компанії «Cambridge Analytica» [5], яка використовувала ці дані для політичного маркетингу. Це призвело до серйозних питань щодо конфіденційності даних та приватності в інтернеті.

Обмеження BCM2711. Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) — це потужний чіп, який часто використовується в різних пристроях, включно з перспективами застосування в безпілотних літальних апаратах (БПЛА). Висока продуктивність та енергоефективність робить його ідеальним вибором для вбудованих систем, де ресурси обмежені та потребується надійність. Однак, незважаючи на ці переваги, BCM2711 має одне значуще обмеження: він не має апаратного прискорення для AES-шифрування. AES, або Advanced Encryption Standard, є одним із найбільш надійних та широко використовуваних алгоритмів шифрування у світі. Відсутність апаратного прискорення AES означає, що всі операції шифрування та дешифрування, які застосовують AES, мають оброблятися програмно, що може призвести до значного зниження швидкості цих операцій. Це може бути особливо проблематичним для БПЛА, які часто потребують швидкого шифрування та дешифрування даних у реальному часі для надійного та безпечного керування.

ОСНОВНА ЧАСТИНА

У межах дослідження здійснено заміри швидкості шифрування та дешифрування для різних алгоритмів на пристрої Raspberry Pi 4 з 4 ГБ оперативної пам'яті. Raspberry Pi 4 використовує процесор Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit, який, як вже було зазначено, не має апаратного прискорення для алгоритмів AES. Результати замірів для алгоритмів xchacha12, xchacha20 та aes-xts за різних частот процесора наведено в таблиці.

З дослідження швидкості шифрування і дешифрування на процесорі Broadcom BCM2711 за різних частот (1600, 1800, 2000 та 2100 MHz), можна дійти кількох головних висновків:

1. Швидкість шифрування і дешифрування нарощується зі збільшенням частоти процесора. Це очікуваний результат, оскільки збільшення частоти процесора зумовлює зростання загальної обчислювальної потужності.

2. XChaCha12 показує найвищу швидкість шифрування та дешифрування за всіх частот, порівняно з xchacha20 та aes-xts. Наприклад, при 2100 MHz xchacha12 має швидкість шифрування 256,4 MiB/s та дешифрування 257,6 MiB/s, порівняно з 215,0 MiB/s та 215,1 MiB/s для xchacha20, і 118,6 MiB/s та 120,9 MiB/s для aes-xts (довжина ключа 256b).

Заміри швидкості шифрування на BCM2711

Частота	Алгоритм	Ключ	Шифрування, MiB/s	Зворотнє, MiB/s
1600 MHz	xchacha12	256b	209,3	209,7
	xchacha20	256b	173,9	173,5
	aes-xts	256b	93,3	95,1
	aes-xts	512b	72,9	73,9
1800 MHz	xchacha12	256b	231,0	232,2
	xchacha20	256b	191,6	192,5
	aes-xts	256b	103,2	105,9
	aes-xts	512b	80,9	82,1
2000 MHz	xchacha12	256b	246,3	245,3
	xchacha20	256b	204,2	205,2
	aes-xts	256b	113,3	115,4
	aes-xts	512b	89,4	90,8
2100 MHz	xchacha12	256b	256,4	257,6
	xchacha20	256b	215,0	215,1
	aes-xts	256b	118,6	120,9
	aes-xts	512b	93,0	94,5

3. AES-XTS має значно меншу швидкість шифрування та дешифрування порівняно з XChaCha12 та XChaCha20. Це може бути особливо критичним для систем, де швидкість є важливим фактором, наприклад систем керування БПЛА у реальному часі.

ВИСНОВКИ

Для систем, де швидкість є важливим фактором, xchacha12, здається, є найефективнішим алгоритмом для використання на процесорі Broadcom BCM2711, незалежно від частоти процесора. Однак важливо зауважити, що хоча ChaCha12 залишається безпечним за даними сучасних досліджень [6], перехід на ChaCha20 може забезпечити більший запас безпеки в разі майбутніх атак, проте це призведе до зниження швидкості. Також перед вибором алгоритму для конкретної системи потрібно брати до уваги інші фактори, зокрема рівень безпеки, пристосованість алгоритму до конкретного застосування та наявність апаратного прискорення.

Здійснений аналіз має допомогти розробникам та інженерам у виборі оптимального алгоритму шифрування для їхніх систем, зважаючи на такі фактори, як швидкість, безпека та апаратні обмеження.

Список використаної літератури

1. ***Forum*** *Raspberry Pi. BCM2837B0 and ARMv8 Crypto Extensions [Електронний ресурс]. URL: https://forums.raspberrypi.com//viewtopic.php?f=63&t=207888*

2. ***Datasheet*** *BCM2711 [Електронний ресурс]. URL:*

https://datasheets.raspberrypi.com/bcm2711/bcm2711-peripherals.pdf

3. ***What*** *Is Data Encryption: Types, Algorithms, Techniques and Methods [Електронний ресурс]. URL:*

https://www.simplilearn.com/data-encryption-methods-article

4. ***CSO.*** *Equifax data breach FAQ: What happened, who was affected, what was the impact? [Електронний ресурс]. URL:*

https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

5. ***Fotis.*** *Case study: Facebook–Cambridge Analytica data breach scandal [Електронний ресурс] URL:*

https://fotislaw.com/lawtify/case-study-on-facebooks-data-breach/

6. ***Springer*** *Link. Improved Key Recovery Attacks on Reduced-Round Salsa20 and ChaCha [Електронний ресурс]. URL:*

https://link.springer.com/chapter/10.1007/978-3-642-37682-5_24

O. I. Barannik

PROBLEMS OF AES ENCRYPTION WITHOUT HARDWARE ACCELERATION ON BROADCOM BCM2711 CHIPS

In today's world, information security plays a critical role in various aspects of our lives. Over the past decade, data encryption has become the primary means of ensuring confidentiality, integrity, and availability of information. Using modern encryption algorithms, we can protect our data from unauthorized access and malicious use.

With the development of technology, single-board computers are becoming more popular and functional. The use of single-board computers can significantly increase the functionality of UAVs. For example, using a single-board computer with real-time video processing capabilities can enable UAVs to perform tasks such as monitoring territories, tracking objects, or even performing search and rescue operations.

However, devices such as unmanned aerial vehicles (UAVs), which require high data processing speeds and low energy consumption, are often limited by the lack of hardware acceleration for encryption algorithms such as AES [1]. This leads to a sharp decrease in encryption and decryption speeds. Such a limitation requires us to search for effective alternatives to the AES algorithm for such devices.

Considering these limitations and the need for alternatives, the purpose of this article is to compare the performance of different encryption algorithms on the Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) 64-bit SoC [2]. We analyze the encryption and decryption speeds for AES-256, AES-512, ChaCha12, and ChaCha20 algorithms. This will allow us to understand which algorithm is most effective for use in UAV control systems and other devices built on Bcm2711 that do not have AES hardware acceleration.

Keywords: encryption; decryption; UAVs; Raspberry Pi 4; AES; ChaCha20; hardware acceleration; ChaCha12; algorithmic efficiency; single-board computers; wireless communications.