# Rust 기술 동향

김상원

https://youtu.be/DpyJIiyYvo4

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

# Rust 관련 연구

- Rust vs C++, a Battle of Speed and Efficiency.

- C++와 Rust로 작성된 코드의 속도와 효율성을 비교 분석한 연구
- 정렬 알고리즘인 Counting Sort와 Bubble Sort 기법을 비교에 사용
- Rust는 컴파일 시간이 짧고 메모리 안전성이 뛰어난 것으로 나타남
- C++과 비교 했을 때 거의 비슷한 성능을 보여줌

| Languages | Memory Used (kb) (Compilation) | Memory Used (kb) (Execution) | Compilation Time (seconds) | Execution Time (seconds) | LOC (Lines of Code) |
|---|---|---|---|---|---|
| Rust | 109392 | 1621 | 0.82s | 0.011s | 26 |
| C++ | 77301 | 1504 | 0.14s | 0.005s | 49 |

**Table 1: Results for Counting Sort Algorithm**

| Languages | Memory Used (kb) (Compilation) | Memory Used (kb) (Execution) | Compilation Time (seconds) | Execution Time (seconds) | LOC (Lines of Code) |
|---|---|---|---|---|---|
| Rust | 112384 | 1584 | 0.655 | 0.003 | 27 |
| C++ | 66576 | 1424 | 0.499 | 0.002 | 38 |

ISSN: 2834-7706

Research Article | *Journal of Mathematical Techniques and Computational Mathematics*

## Rust vs C++, a Battle of Speed and Efficiency

**Vincent Ng***

*Computer Science St Joseph International School Kuala Lumpur, 57000, Malaysia.*

*Corresponding Author
Vincent Ng, Computer Science St Joseph International School Kuala Lumpur, 57000, Malaysia.

**Submitted:** 2023, May 18; **Accepted:** 2023, Jun 17; **Published:** 2023, June 21

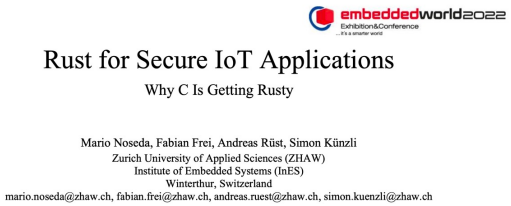
**Citation:** Vincent, Ng. (2023). Rust vs C++, a Battle of Speed and Efficiency. *J Math Techniques Comput Math, 2*(6), 216-220.

**Abstract**

*This study compares the performance of two excellent options for system-level development, the programming languages C++ and Rust. Through a series of tests and experiments using socket servers and various algorithms, this experiment analyses the speed and efficiency of code written in each language by looking at variables like memory management, and compilation times. The findings reveal that Rust has a number of advantages over C++, including quicker compilation times, improved memory safety, and in many situations equivalent or better performance. C++ still performs exceptionally well in several fields, nevertheless, such as low-level hardware programming and backward compatibility. Overall, the results indicate that Rust is a strong candidate for systems programming jobs, especially for new projects or those requiring a high level of performance and security.*

# Rust 관련 연구

- Rust for secure iot applications: why c is getting rusty.




- Rust는 IoT 애플리케이션 개발에서 안전성과 효율성을 크게 향상시킬 수 있는 기능을 제공
- 외부 함수 인터페이스(FFI)를 활용하여 기존의 C/C++ 시스템과의 통합을 용이하게 하며, 이는 개발자들에게 더욱 유연한 프로그래밍 환경을 제공 가능케 함
- Rust는 컴파일 시간에 대부분의 메모리 버그를 탐지하고 수정할 수 있기 때문에, 런타임 중 발생할 수 있는 예외 상황을 크게 줄이고, 특히 네트워크 연결이 제한적이거나 유지보수가 어려운 원격 IoT 디바이스에서 이는 매우 중요
- IoT에 사용되는 임베디드 기기 시스템 특성상 메모리 취약점을 통해 기기가 손상될 수 있기에 메모리 안정성을 보장하는 Rust를 사용함으로써 그 한계를 최소화 할 수 있음
- 성능에 있어서 C언어와 큰 차이가 없었는데 이는 배터리를 사용하는 기기에서 특히 중요함

TABLE IV: RELATIVE DIFFERENCE IN EXECUTION TIME FOR CRYPTOGRAPHIC ALGORITHMS WHEN SWITCHING FROM MBEDTLS (C) TO RUSTCRYPTO (RUST).

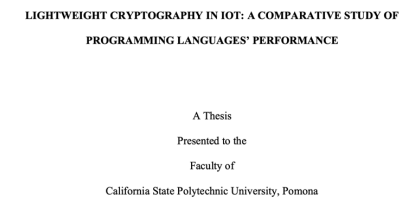
| Algorithm | From C to Rust |
|---|---|
| SHA256 (16 B) | - 13 % |
| SHA256 (64 KiB) | - 9 % |
| AES128-CCM (16 B) | + 145 % |
| AES128-CCM (64 KiB) | + 73 % |
| AES128-GCM (16 B) | + 101 % |
| AES128-GCM (64 KiB) | + 20 % |
| CHACHA20-POLY1305 (16 B) | - 53 % |
| CHACHA20-POLY1305 (64 KiB) | - 52 % |

TABLE V: SCOREBOARD FOR THE COMPUTER LANGUAGE BENCHMARKS GAME.

| Language | Points |
|---|---|
| C++ | 21 |
| Rust | 20 |
| C | 19 |

# Rust 암호구현 동향

- LIGHTWEIGHT CRYPTOGRAPHY IN IOT: A COMPARATIVE STUDY OF PROGRAMMING LANGUAGES' PERFORMANCE

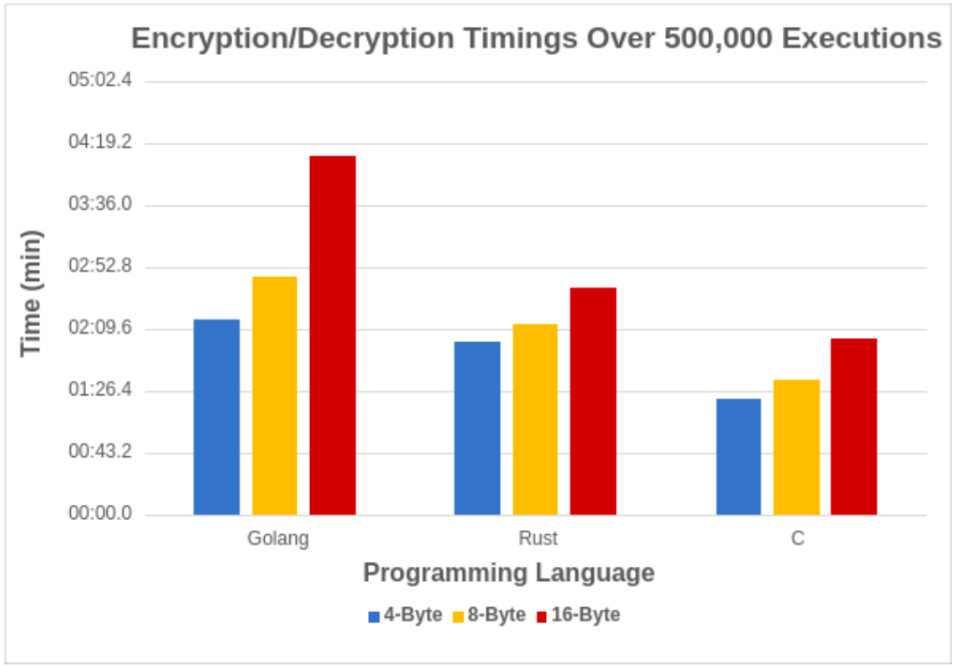

LIGHTWEIGHT CRYPTOGRAPHY IN IOT: A COMPARATIVE STUDY OF
PROGRAMMING LANGUAGES' PERFORMANCE

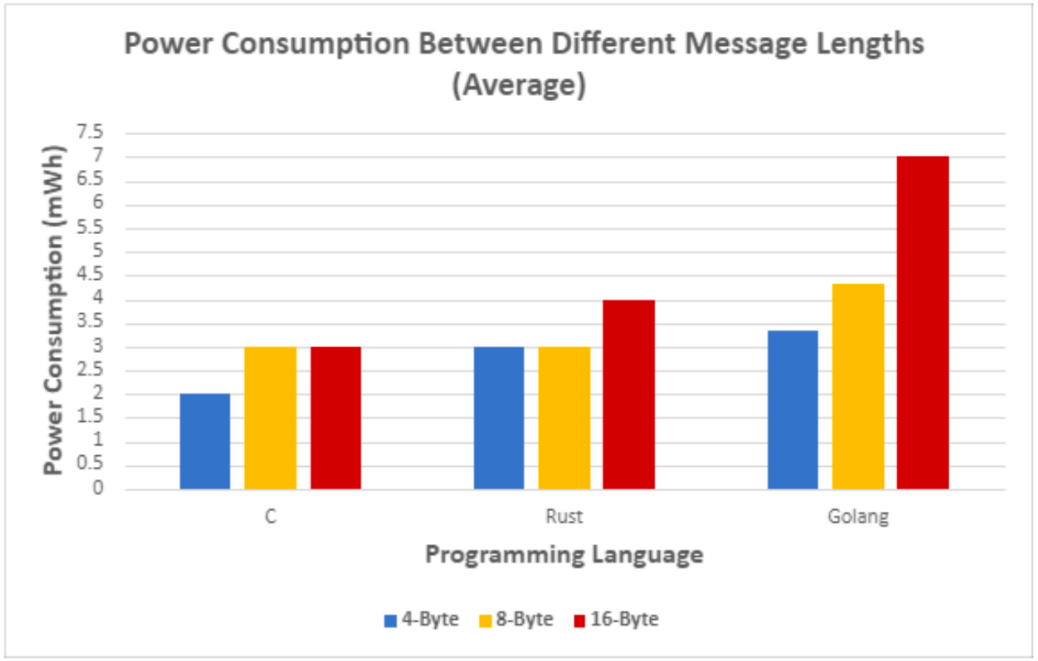
A Thesis
Presented to the
Faculty of
California State Polytechnic University, Pomona

- TinyJAMBU라는 경량 암호화 알고리즘을 중심으로 여러 프로그래밍 언어의 성능을 비교 분석한 논문
- TinyJAMBU는 리소스가 제한된 IoT 환경에서 사용하기 위해 설계된 알고리즘으로, 낮은 메모리와 처리 능력 요구 사항에도 불구하고 높은 보안성을 제공
- 이 연구에서 Rust, C, 그리고 Go 언어로 구현된 TinyJAMBU의 성능을 비교한 결과, C와 비교했을 때, Rust는 전력 소비 면에서는 C와 거의 비슷하고, 성능 면에서는 약간 뒤처졌음
- 이를 다르게 보자면 Rust가 C와 비슷한 자원을 가지고 비슷한 속도를 내며 메모리 안전성까지 가질 수 있다는 것을 의미함

# Rust 암호구현 동향

- LIGHTWEIGHT CRYPTOGRAPHY IN IOT: A COMPARATIVE STUDY OF PROGRAMMING LANGUAGES' PERFORMANCE



# Rust 암호구현 동향

- RUST-Encoded Stream Ciphers on a RISC-V Parallel Ultra-Low-Power Processor.
- 사이버 물리 시스템(CPS)와 사물인터넷(IoT)의 보안과 관련된 RISC-V 병렬 저전력 아키텍처(PULP)를 활용한 연구
- 특히, 이 연구에서는 비디오 스트림의 보안을 강화하기 위해 스트림 암호화 기법을 적용하고, Rust 코드 안전성을 활용하여 ChaCha20 및 AES-CTR 스트림 암호화 알고리즘을 효율적으로 구현
- Rust의 외부 함수 인터페이스(FFI)를 사용하여 기존의 C 언어로 작성된 PULP SDK와의 연동을 가능하게 하며, PULP 아키텍처의 병렬 처리 능력을 최대한 활용하여 암호화 알고리즘의 성능을 향상시킴
- 이로 인해, PULP 아키텍처에서 스트림 암호화를 구현할 때 발생할 수 있는 보안 취약점을 최소화할 수 있게 됨
- 결과적으로, 이 연구는 저전력이면서 고성능을 요구하는 임베디드 시스템에서의 스트림 암호화 구현에 있어 Rust의 유용성을 입증함

# Rust 암호구현 동향

- High-Assurance, High-Speed Post-Quantum Cryptography in Safe Rust.
- 양자내성암호 분야에서도 Rust가 사용 되는 중
- 이 연구에서는 Jasmin으로 구현된 기존의 Kyber 알고리즘을 Rust로 확장하여, Rust 프로그램에서 안전하게 호출할 수 있는 고효율의 Kyber 라이브러리(RjKyber)를 제공함
- 이 과정에서 Jasmin 구현이 Rust에서 호출되면서 두 언어의 보안 제약을 유지하는 방법 조사
- 이를 통해 얻은 통합의 효율성, 안전성 및 사용 용이성은 단독 언어로는 달성할 수 없는 수준


FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

High-Assurance, High-Speed Post-Quantum Cryptography in Safe Rust

Leonardo Moura

U.PORTO
FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

Mestrado em Engenharia Informática e Computação

Supervisor: Prof. Dr. Rui Maranhão

Cosupervisor: Prof. Dr. Manuel Barbosa

July 31, 2022

# Rust 암호구현 동향

- High-Assurance, High-Speed Post-Quantum Cryptography in Safe Rust.

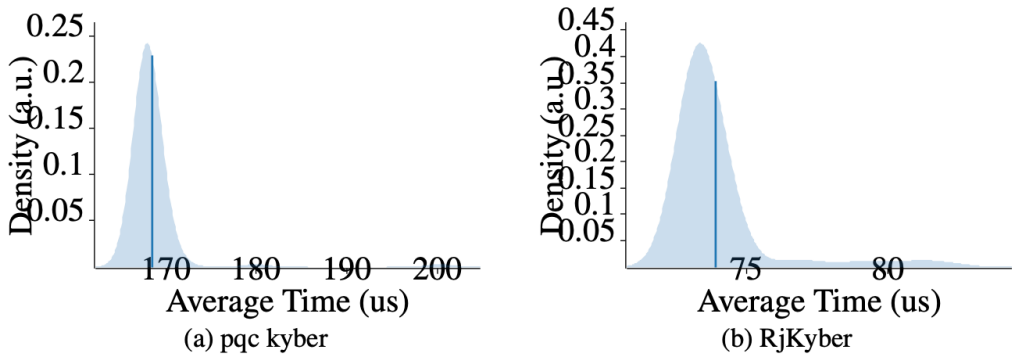



Figure 6.4: Keygen functions comparison

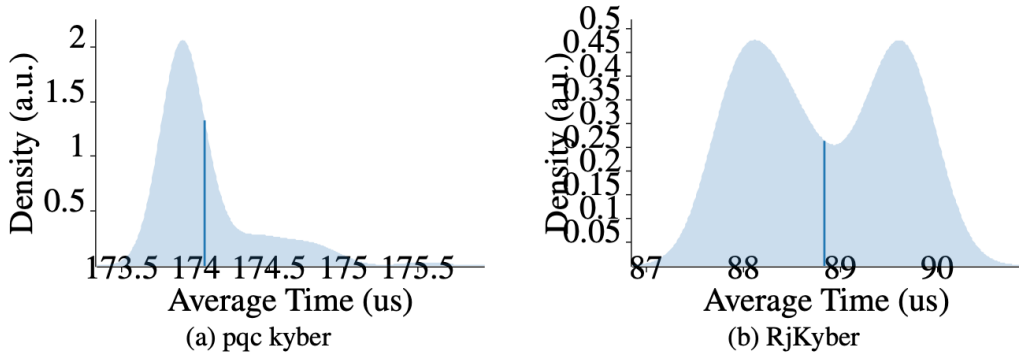



Figure 6.5: Encapsulation functions comparison

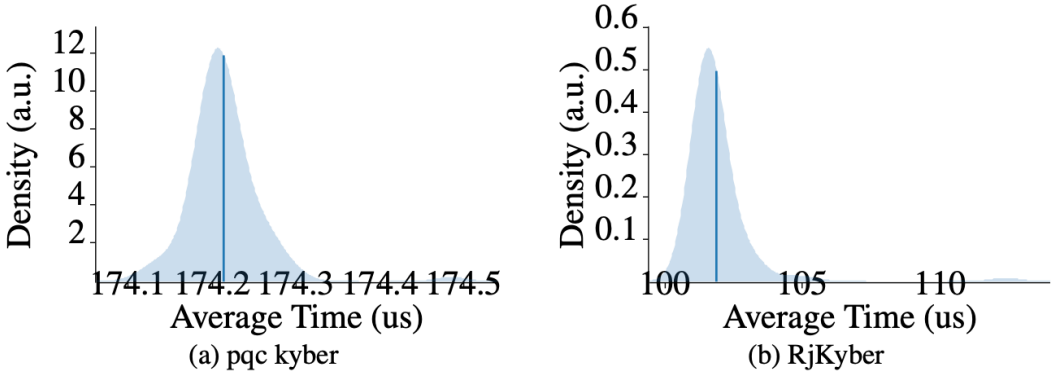



Table 6.2: Mean execution times of pqc kyber and RjKyber

| Function | pqc kyber (us) | RjKyber (us) |
|---|---|---|
| Keygen | 168.51 | 73.882 |
| Encapsulation | 174.06 | 88.832 |
| Decapsulation | 174.21 | 101.90 |

# Rust 암호구현 동향

- Analysis and Contributions to a Post-Quantum Cryptography Library written in Rust for a ARM Cortex-M4 board
- ARM Cortex M4 마이크로컨트롤러에서 효율적이고 실용적인 PQC 솔루션을 제공하기 위해 Rust 프로그래밍 언어로 작성된 특정 Kyber 라이브러리를 선택하는 경우도 있음
- Rust를 주로 ARM Cortex M4 마이크로컨트롤러에 양자내성암호 라이브러리를 통합하고, 이를 통해 양자 위협에 대응할 수 있는 보안을 강화하는 방식으로 사용
- 이 연구는 라이브러리에 대한 개선과 코드 성숙도 측면에서의 기여도를 제공하며, Kyber KEM (키 캡슐화 메커니즘)을 중심으로 분석을 집중하고 있음


POLITECNICO DI TORINO
Master's Degree in Computer Engineering
Politecnico di Torino
1859
Master's Degree Thesis
Analysis and Contributions to a Post-Quantum Cryptography Library written in Rust for a ARM Cortex-M4 board
Supervisors
Prof. ANTONIO JOSE' DI SCALA
Dott. Guido BERTONI
Dott. Maria Chiara MOLTENI
Candidate
Francesco MEDINA
April 2024

# Q & A