UNIVERSITY OF INFORMATION TECHNOLOGY
FACULTY OF COMPUTER NETWORK AND COMMUNICATION

CRYPTOGRAPHY

Report Lab 5

Digital Signature with Crypto++/OpenSSL

Lecturer:	Nguyễn Ngọc Tự
Class:	NT219.O21.ANTT.2
Student:	Trần Thế Hữu Phúc
Student ID Number:	22521143

Hồ Chí Minh City, June 2024

1. Hardware Resources

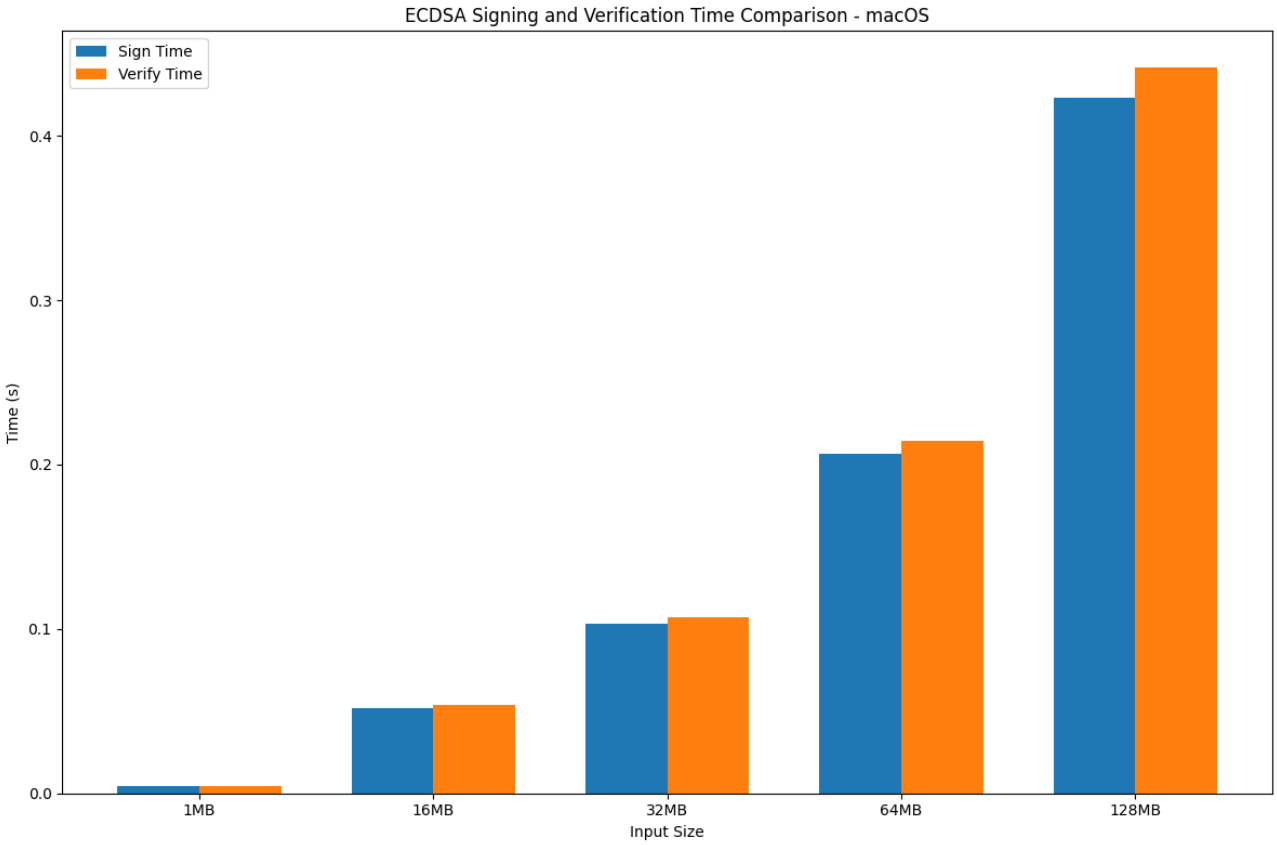
Device	MacBook Pro
Chip	Apple M1 • 8-core CPU • 8-core GPU • 16-core Neural Engine
Memory	8GB LPDDR4
Storage	256GB SSD
Operating Systems	• macOS 14.5 Sonoma • Windows 11 Pro Version 23H2 • Ubuntu 22.04.4 LTS

2. Computation performance on macOS, Windows and Linux

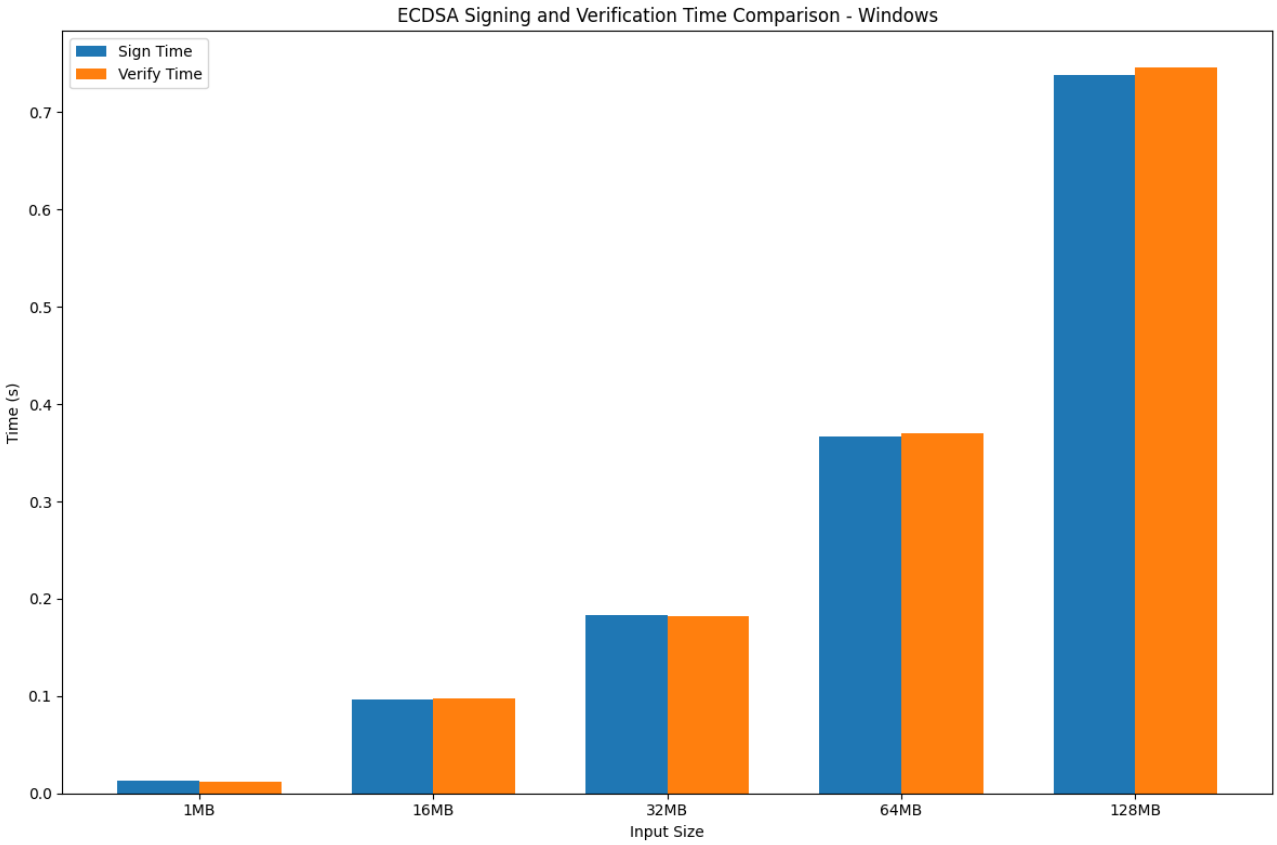
2.1. ECDSA

ECDSA on all platforms (miliseconds)						
OS		Input Size				
		1MB	16MB	32MB	64MB	128MB
macOS	Sign	0.004	0.052	0.103	0.207	0.423
	Verify	0.004	0.054	0.107	0.214	0.442
Windows	Sign	0.013	0.097	0.183	0.367	0.738
	Verify	0.012	0.098	0.182	0.370	0.746
Linux	Sign	0.014	0.145	0.287	0.576	1.106
	Verify	0.012	0.141	0.286	0.572	1.100

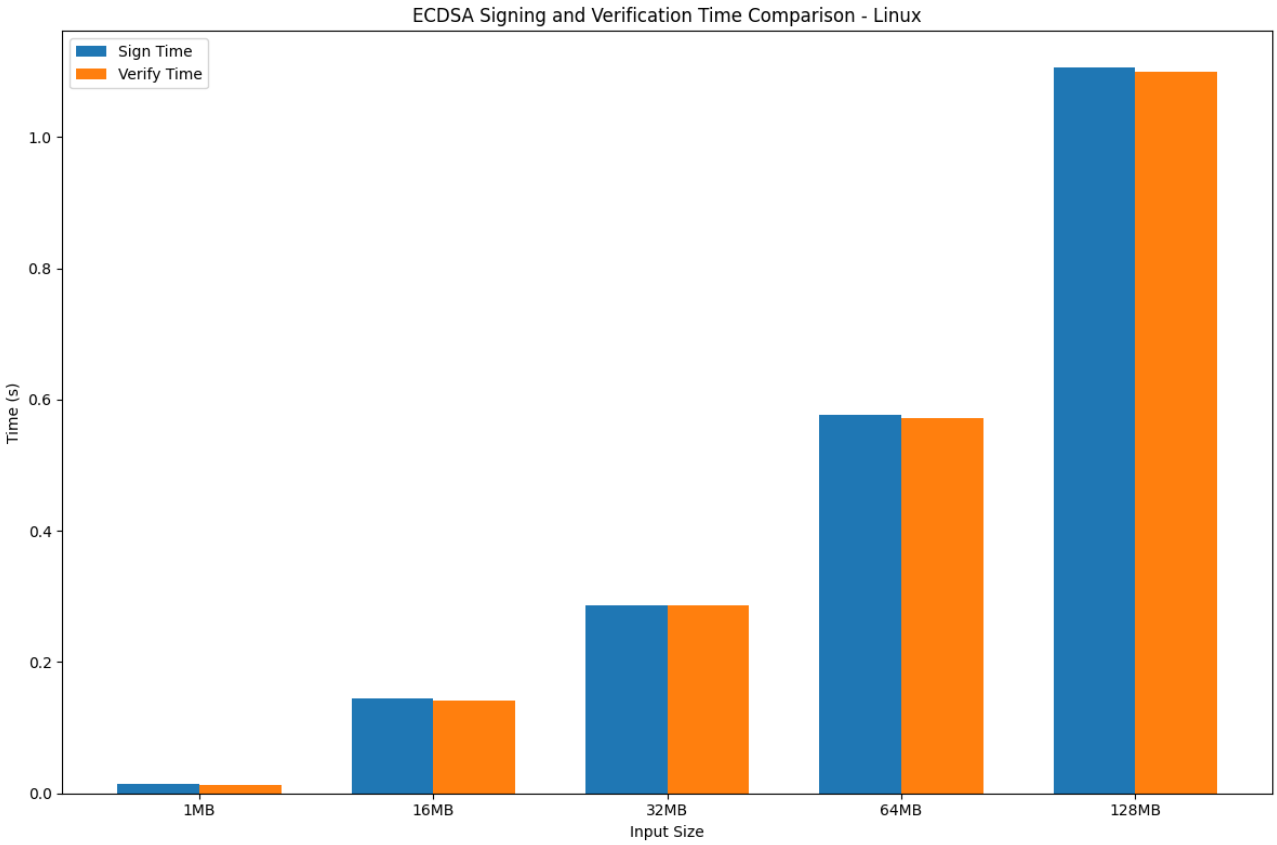
- **ECDSA on macOS:**



- **ECDSA on Windows:**



- **ECDSA on Linux:**



⌥ Phân tích và so sánh

- **Thời gian xử lý tăng tuyến tính:** Cả ba hệ điều hành đều có sự tăng thời gian xử lý khi kích thước tệp tin tăng, nhưng tốc độ tăng này là khác nhau. macOS tăng chậm nhất, tiếp theo là Windows và Linux tăng nhanh nhất.
- **Hiệu năng:**
  - **macOS**: macOS có thời gian xử lý nhanh nhất so với Windows và Linux ở tất cả các kích thước tệp tin. Thời gian ký và xác minh tăng lên một cách tương đối đồng đều khi kích thước tệp tăng lên. Thời gian ký và xác minh gần như tương đương nhau cho tất cả các kích thước tệp tin nhưng có chênh lệch lớn hơn so với các hệ điều hành khác (Sign < Verify).
  - **Windows**: Windows có thời gian xử lý chậm hơn macOS nhưng nhanh hơn Linux. Thời gian ký và xác minh cũng tăng lên một cách đồng đều khi kích thước tệp tăng lên. Thời gian ký và xác minh cũng rất gần nhau, nhưng có một số chênh lệch nhỏ (Sign < Verify).
  - **Linux**: Linux có thời gian xử lý chậm nhất so với macOS và Windows. Thời gian ký và xác minh tăng lên nhanh chóng khi kích thước tệp tăng lên. Thời gian ký và xác minh cũng tương đương nhau nhưng có chênh lệch nhỏ hơn so với các hệ điều hành khác (Sign > Verify).

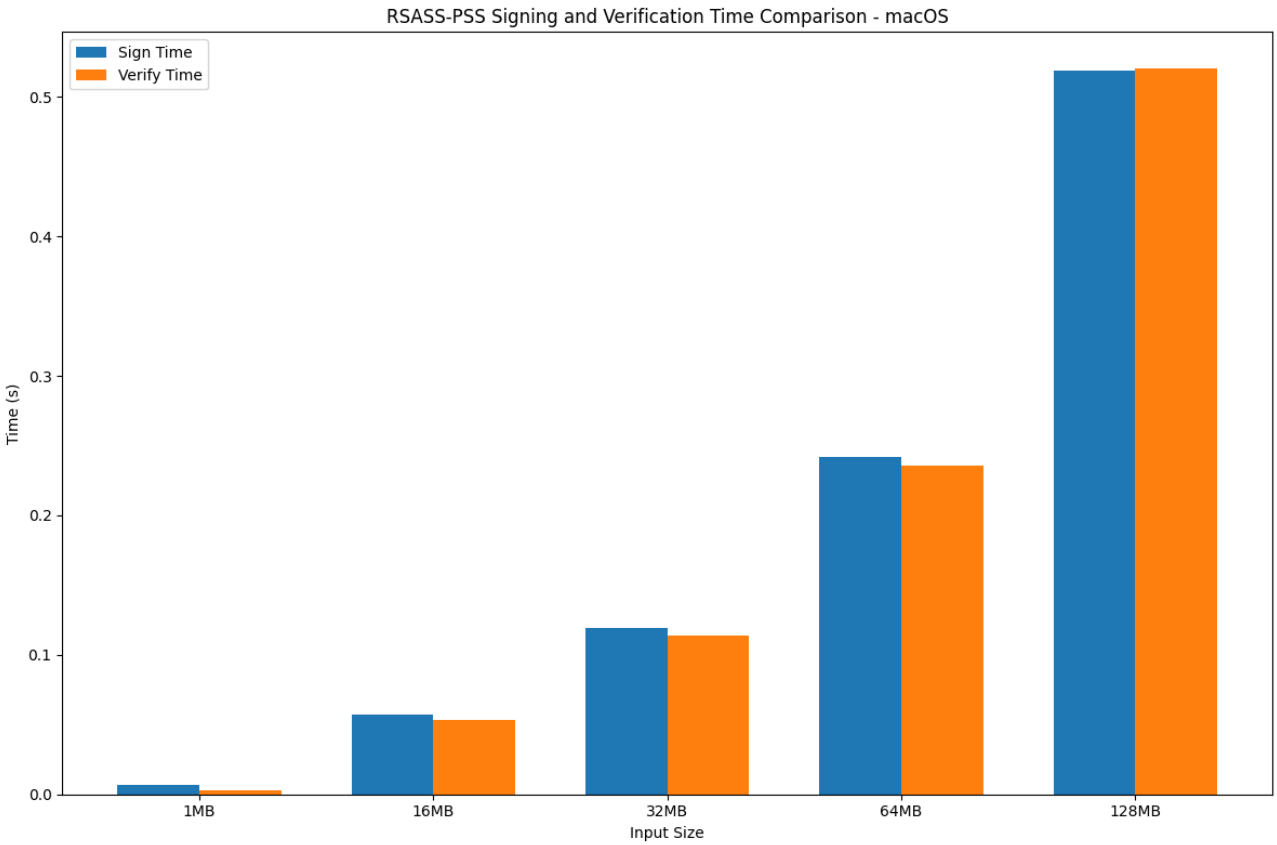
=> Kết luận:

- Trong cả ba hệ điều hành, thời gian ký và xác minh tương đối gần nhau, cho thấy sự nhất quán trong hiệu suất xử lý.
- macOS có hiệu suất tốt nhất cho cả ký và xác minh, tiếp theo là Windows và cuối cùng là Linux.

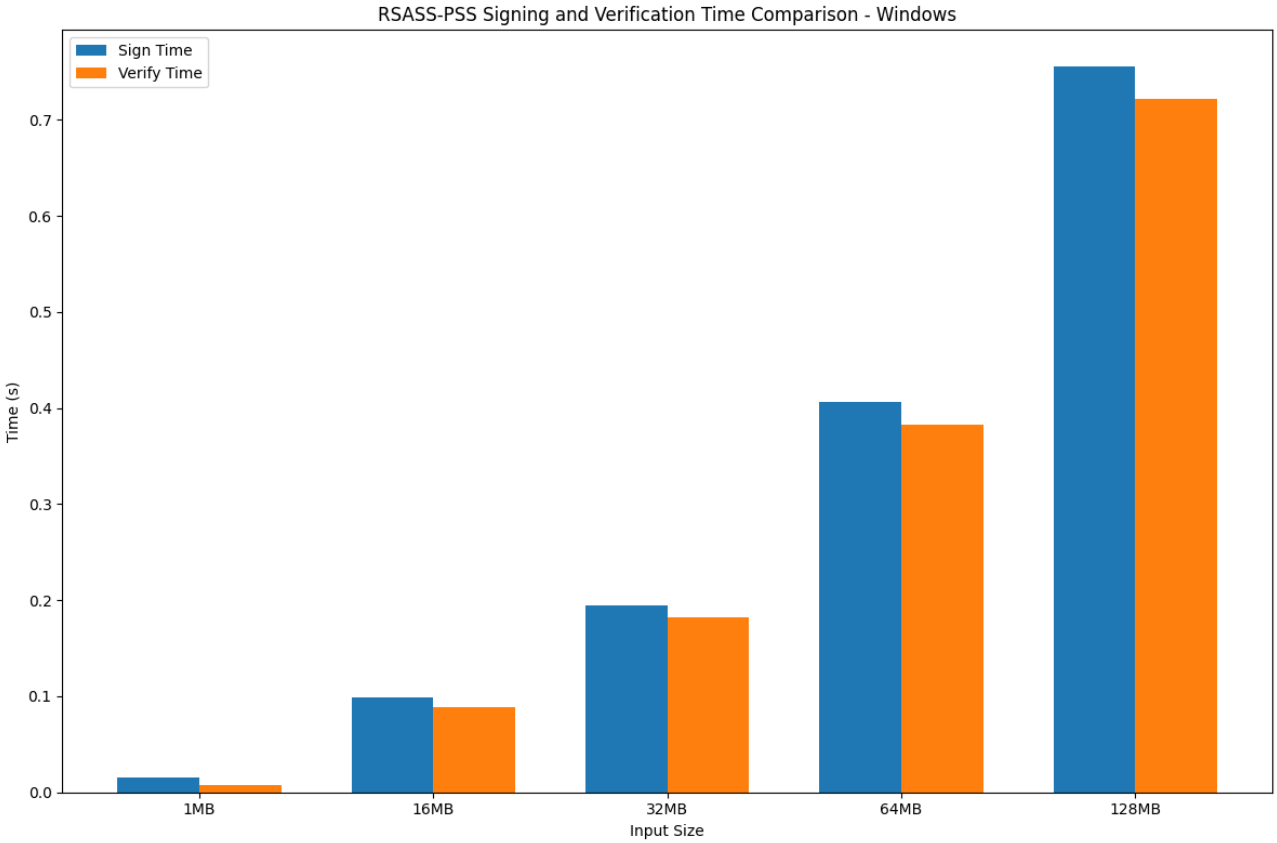
2.2. RSASS-PSS

RSASS-PSS on all platforms (miliseconds)						
OS		Input Size				
		1MB	16MB	32MB	64MB	128MB
macOS	Sign	0.006	0.057	0.120	0.242	0.519
	Verify	0.003	0.054	0.114	0.236	0.520
Windows	Sign	0.015	0.099	0.195	0.407	0.756
	Verify	0.007	0.089	0.182	0.383	0.722
Linux	Sign	0.017	0.147	0.286	0.574	1.112
	Verify	0.010	0.141	0.278	0.570	1.098

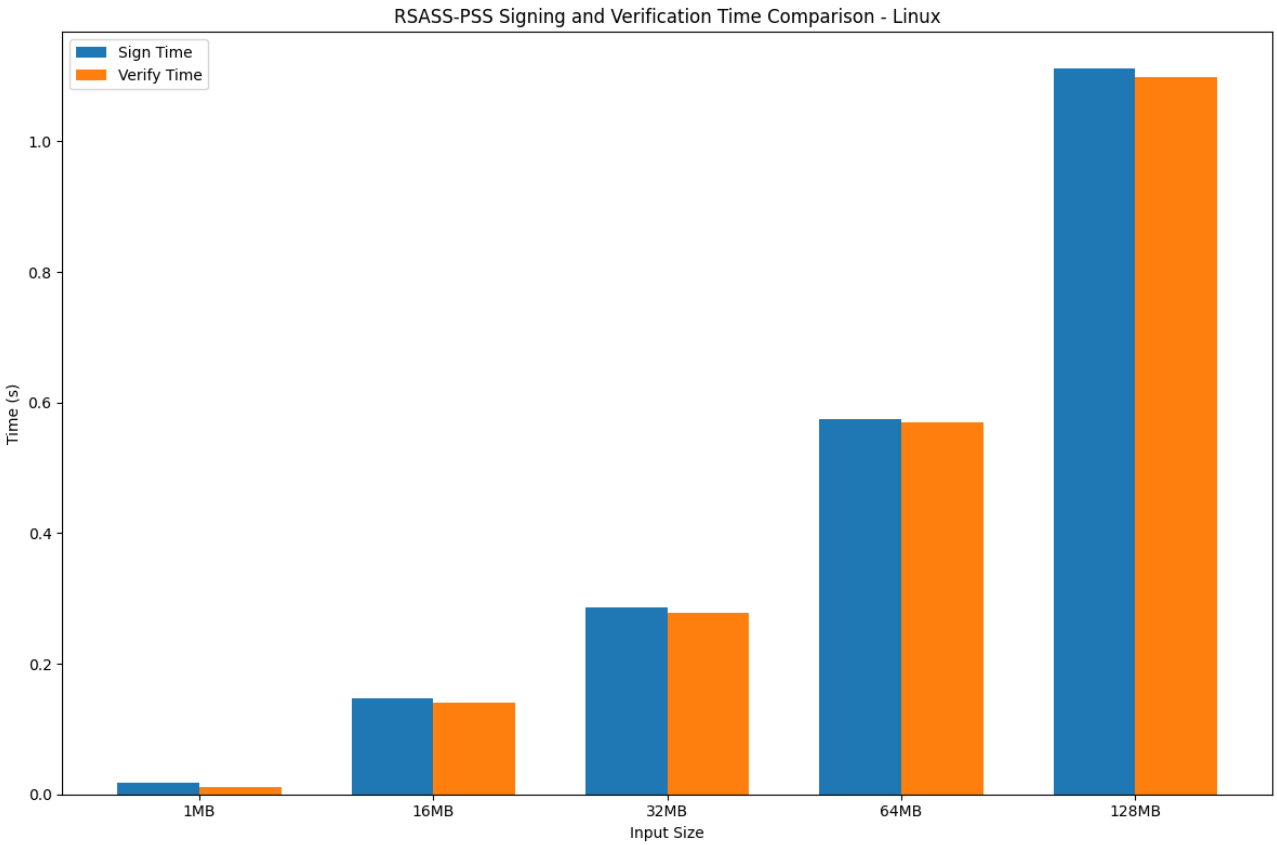
- **RSASS-PSS on macOS:**



- **RSASS-PSS on Windows:**



- **RSASS-PSS on Linux:**



⌥ Phân tích và so sánh

- **Thời gian xử lý tăng tuyến tính:** Cả ba hệ điều hành đều có sự tăng thời gian xử lý khi kích thước tệp tin tăng. Thời gian ký có vẻ chênh lệch hơn thời gian xác minh ở cả 3 nền tảng.
- **Hiệu năng:**
  - **macOS**: macOS có thời gian xử lý nhanh nhất so với Windows và Linux ở tất cả các kích thước tệp tin. Thời gian ký và xác minh rất gần nhau, đặc biệt là khi kích thước tệp tăng lên.
  - **Windows**: Windows có thời gian xử lý chậm hơn macOS nhưng nhanh hơn Linux. Thời gian ký và xác minh cũng tăng lên một cách đồng đều khi kích thước tệp tăng lên. Thời gian ký và xác minh có sự chênh lệch lớn hơn so với macOS.
  - **Linux**: Linux có thời gian xử lý chậm nhất so với macOS và Windows. Thời gian ký và xác minh cũng gần tương đương nhau, nhưng có chênh lệch rất nhỏ.

=> Kết luận:

- Trong cả ba hệ điều hành, thời gian ký và xác minh tương đối gần nhau, nhưng macOS cho thấy sự nhất quán và hiệu suất tốt nhất tiếp theo đó là Windows và cuối cùng là Linux.