Momo Hirose
CS 360
April 22nd, 2024

# GPGPUs in Cryptography

- What is cryptography?

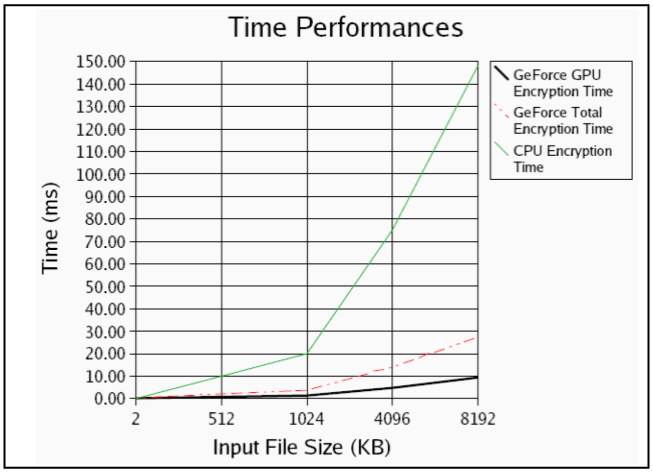
Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages (Wikipedia, 2024). The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce (Fortinet, 2024).

- Problem in this domain

As the number of computer users continues to grow, the number of cyber-attacks to steal data and invade privacy is of paramount importance. A group of applications use the Advanced Encryption Standard (AES), which is the most widely adopted modern symmetric key encryption standard, to encrypt data for security reasons. This primarily affects enterprises and businesses that ultimately handle user data. However, many implementations of the AES algorithm consume large amounts of CPU power and do not meet throughput requirements (Jadhav, et al., 2023).

- GPUs as a solution

To solve this problem, GPUs dedicated to parallel applications can be used to achieve speedups through massive parallelism. These allow parallel operations to be performed much faster than the CPU, ultimately increasing throughput and reducing resource consumption to some extent (Jadhav, et al., 2023). Existing research has demonstrated that GPUs can act as an efficient cryptographic accelerator faster than CPUs by parallelizing the encryption/decryption process (Manavski, 2007).



Momo Hirose
CS 360
April 22nd, 2024

## References

Fortinet. (2024). What is Cryptography? Retrieved from https://www.fortinet.com/resources/cyberglossary/what-is-cryptography#:~:text=Cryptography%20is%20the%20process%20of,%2C%20computer%20passwords%2C%20and%20ecommerce

Jadhav, S., Patel, U., Natu, A., Patil, B., & Palwe, S. (2023). Cryptography Using GPGPU. In G. Rajakumar, K. L. Du, & Á. Rocha (Eds.), Intelligent Communication Technologies and Virtual Mobile Networks. ICICV 2023. Lecture Notes on Data Engineering and Communications Technologies (Vol. 171). Springer, Singapore. https://doi.org/10.1007/978-981-99-1767-9_23

Manavski, S. A. (2007, November). CUDA compatible GPU as an efficient hardware accelerator for AES cryptography. In *2007 IEEE International Conference on Signal Processing and Communications* (pp. 65-68). IEEE.

Wikipedia. (2024). Cryptography. Retrieved from https://en.wikipedia.org/wiki/Cryptography