A Study on Processors for use in Cryptography

[1]Reena Kulkarni, [2]Hemapriya M, [3]Tejaswini G V

[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor
[1]Department of Electronics and Communication Engineering
[1]K. S. School of Engineering and Management, Bengaluru, India
[1]reenadk@gmail.com, [2]hemapriya@kssem.edu.in, [3]tejaswini.gv@kssem.edu.in

***Abstract*— Cryptographic algorithms demand high computational power, higher speed of processing, efficiency, and security, which has led to the development of specialized processors optimized for cryptographic operations. As the demand for secure data transmission and storage is increasing across sectors, selecting the right hardware to handle cryptographic operations is very essential. This study provides a view of various processor features, ranging from general-purpose central processing units (CPUs), to specialized processors like graphics processing units (GPUs), Application Specific Integrated Circuits (ASICs), secure processors and field programmable gate arrays (FPGAs) and the many challenges involved for implementing/running cryptographic algorithms.**

***Index Terms*—Cryptographic algorithms, processors, CPU, GPU, ASIC, FPGA.**

I. INTRODUCTION

With the growing demand for secure communications, data protection, and blockchain technologies, processors designed or for cryptographic tasks have emerged as vital components in both consumer and enterprise systems. Cryptographic algorithms often demand substantial computational resources due to their complexity. The selection of an appropriate processor is significant in ensuring optimal performance and resilience against attacks. Cryptographic algorithms that include encryption, decryption, hashing, and digital signature generation, depend heavily on the processing power of hardware to execute complex mathematical operations at high speed with lowest possible latency.The efficiency and security of cryptographic operations are largely influenced by the type of processor architectural features, hardware acceleration techniques, and implementation trade-offs relevant to secure and efficient cryptographic processing. Over the years, various types of processors, including general-purpose CPUs, GPUs, FPGAs, and ASICs, have been employed in cryptography, each offering distinct advantages and challenges.This paper discusses the various hardware available for cryptographic implementations and their real world applications [1][2].

II. NEED FOR SEPARATE HARDWARE FOR CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithms play a crucial role in securing data, ensuring confidentiality, integrity, and authenticity in digital communications. Further, these algorithms perform complex mathematical operations which, in turn require high-speed processing that can be inefficient or insecure when performed solely by general-purpose processors. The cryptographic algorithms can be run on several types of processors, each with different strengths and use cases depending on the specific cryptographic task (e.g., encryption, decryption, hashing, digital signatures).

Cryptographic algorithms, such as AES (Advanced Encryption Standard), RSA (Rivest, Shamir, Adleman), ECC (Elliptic Curve Cryptography), and SHA (Secure Hash Algorithm), are computationally intensive and often involve operations like large integer arithmetic, modular exponentiation, and finite field arithmetic, which can be inefficient and overloading on general-purpose CPUs[3],[4]. Furthermore, implementing cryptographic functions purely in software exposes systems to timing attacks, power analysis, and other side-channel attacks due to the predictable behavior and shared resources of conventional processors. Also, software alone might be too slow, especially for real-time or high-volume use. To mitigate these risks and meet performance requirements, dedicated cryptographic hardware is employed [5].

Hardware components such as cryptographic accelerators, secure elements, and hardware security modules (HSMs) are specifically designed to perform cryptographic operations efficiently while incorporating physical and logical protections against tampering, fault injection, side-channel leakage, compliance and certification. These dedicated units often include secure key storage, hardware random number generators (TRNGs), and isolation mechanisms, ensuring that sensitive operations are executed in a trusted environment [6]. As a result, the use of separate cryptographic hardware not only enhances performance but also significantly strengthens the overall security posture of modern computing systems.

Section III discusses about the processors available for implementing cryptographic functions with their advantages, applications and disadvantages.

III. PROCESSORS FOR CRYPTOGRAPHIC ALGORITHMS

General purpose central processing units (CPUs): Whenever flexibility and ease of development are significant, general-purpose CPUs can efficiently execute cryptographic algorithms, like AES, RSA, SHA, and ECC [7]. Processors from manufacturers like AMD or ARM are widely available and support a broad range of applications, making them a practical platform for cryptographic tasks such as, data encryption/decryption, digital signatures, hashing functions and key generation and management [8]. Hardware accelerators coupled with CPUs boost up the overall performance of the system. Algorithms used in the accelerators help in memory optimization processes.

The real world applications where general purpose CPUs are used for cryptographic operations include web security, data encryption in cloud services, mobile security, enterprise security, digital signature verification, blockchain, etc.

Graphic Processing Units (GPUs): Originally designed to accelerate image rendering and graphical computations, GPUs have evolved into powerful parallel processors capable of handling a wide variety of general-purpose tasks. Their architecture, composed of thousands of smaller, efficient cores designed for parallel execution, makes them especially well-suited for many cryptographic algorithms. Tasks such as encryption, decryption, hashing, and key derivation, which involve repetitive operations on large datasets

or many independent data blocks, can be significantly accelerated using GPU computing [9]. This capability has been harnessed in a wide range of applications—from password recovery and digital forensics to blockchain mining and zero-knowledge proof generation. GPUs also present unique challenges in the context of cryptographic security, including concerns around side-channel attacks, memory management, and determinism [10], [11].

The algorithms supported by GPUs include Symmetric ciphers like AES, ChaCha20, Hash functions like SHA-1, SHA-256, SHA-512, Bcrypt, Scrypt, Argon2, Asymmetric ciphers like ECC, RSA and Key derivation like PBKDF2 (password-based key derivation function 2), Bcrypt, Scrypt.

The real world applications where GPUs execute cryptographic operations include cryptocurrency mining, password cracking and cryptanalysis, encryption and decryption in virtual private networks (VPNs), homomorphic encryption, zero knowledge proofs (ZKPs), digital signature generation and verification, etc.

Application-Specific Integrated Circuits (ASICs): ASICs are customized hardware solutions for executing cryptographic algorithms at unparalleled speeds and with extremely low power consumption. Unlike general-purpose CPUs or GPUs that are designed to handle a wide range of tasks, ASICs are custom-built for particular functions only. In cryptography, ASICs can be designed to accelerate execution of algorithms like AES, RSA, ECC, SHA, and many other [12]. These dedicated hardware solutions are highly optimized for specific operations, making them ideal for high-throughput, low-latency cryptographic tasks in environments where performance and energy efficiency are most significant. The various cryptographic algorithms implemented using ASICs include AES, RSA, ECC, SHA, PBKDF2, Bcrypt and. Scrypt [13].

The real world applications where ASICs are employed to secure data are blockchain mining, Secure Hardware Modules (HSMs), encryption acceleration in data centers, smart cards & embedded devices, etc. ASICs have become prominent in specialized areas like blockchain mining, where their ability to execute hash functions at massive scales (like the SHA-256 for Bitcoin) provides a significant performance advantage over general-purpose processors.

Secure Processors: Secure processors are hardware components designed with built-in security features to resist physical and logical tampering, defend side channel attacks, fault injections and reverse engineering. Secure processors enhance protection by offering, isolated execution environments, secure key storage and management, protection against physical tampering, hardware acceleration for cryptographic functions and resistance to side-channel attacks. Secure processors apart from implementing the cryptographic functions also optimize them. The various algorithms supported on secure processors include symmetric cryptographic algorithms like AES, DES, RC4, etc., asymmetric algorithms like RSA, ECC, Diffie-Hellman, etc. Hashing algorithms like SHA, PBKDF2, Bcrypt, Scrypt, etc., and post-quantum cryptography [14], [15].

The real world applications where secure processors are used include PCs, smartphones, Internet of Things (IoT) devices, servers where digital signatures on firmware and OS components are verified; secure payments and digital wallets to protect payment credentials, biometric data, and transaction integrity; cloud key management and data encryption, digital signatures and certificates, biometric authentication, etc.

Field Programmable Gate Arrays (FPGAs): FPGA is a type of semiconductor device that can be programmed or reprogrammed to perform specific tasks for applications. Unlike traditional microchips, which are designed to perform fixed functions, an FPGA allows users to configure its logic and routing to meet the needs of their application. FPGAs are important for a variety of reasons, mainly because they offer unique advantages in terms of flexibility, speed, and parallel processing. An interesting application of FPGA is in the field of cryptography to meet the growing computational demands of encryption, decryption, and key management. FPGAs can implement cryptographic algorithms in hardware, enabling parallel processing, can update or change algorithms after deployment, provide low latency and as well support evolving standards [16].

FPGAs implement cryptographic algorithms like AES, DES, RSA, ECC, RC4, SHA, in secure protocol implementations like Transport Layer Security (TLS)/ Secure Sockets Layer (SSL) offload, Internet protocol Security (IPsec) and Virtual Private Networks (VPNs).The real world applications where FPGAs are used for cryptographic operations include blockchain mining, military and aerospace communication, hardware security modules (HSMs) and Embedded Systems & IoT [17].

Table 1 summarizes the features of the above mentioned processors for different parameters. As seen in Table 1, FPGA seems quite advantageous when research and experimentation is to be carried out because of its reprogrammable feature that ensures long-term relevance as cryptography evolves, along with cost considerations. FPGAs can be more energy efficient than CPU/GPUs for certain operations. Also, in certain cases, GPUs and FPGAs give better performance than CPUs alone. Further, the accelerators based on FPGA or ASIC architecture work with high speeds than when working with shared memories.

Table 1: Features of various processors.

Processor	Flexibility	Performance	Cost	Power Efficiency	Security
CPU	High	Moderate	Low	Low	Moderate
GPU	Low	High (data-parallel)	Moderate	Low	Low
ASIC	None	Very High	Very High	Very High	Very High
FPGA	High	High (parallel processing)	Moderate	High	High

IV. Challenges in selecting a processor

Cryptographic algorithms, particularly asymmetric ones like RSA and ECC, are computationally intensive and often require specialized processing capabilities. In selecting an appropriate processor for cryptographic workloads, a multifaceted decision must be made taking into account performance, security, cost, and adaptability features offered by the processor [18], [19]. The following are the key challenges encountered during the processor selection process:

1. Performance and power trade-off: High-performance processors typically consume more power, making them unsuitable for constrained environments such as embedded systems and IoT devices. Maintaining a balance between sufficient computational throughput and energy efficiency is a core challenge.
2. Hardware Acceleration: As all processors do not include built-in support for AES, SHA, or public-key primitives, and the dependence on software implementations can lead to considerable performance bottlenecks.
3. Algorithm support: Asymmetric and symmetric algorithms possess different computational characteristics, hence a generic processor may not be efficient to implement multiple algorithms.
4. Support for scalability and customization: Processor chosen must support latest updates and also must be customizable for inclusion/exclusion of features.
5. Cost versus the capability: High capacity or performance equipped processors cost more, which can be hurdle for budget constrained application areas like IoT.

V. Conclusion

Selection of an appropriate processor for cryptographic operations involves complex decision that includes balancing performance, power efficiency, security, cost, and compatibility. As secure communications, digital identity, and data protection needs are increasing, processors must not only offer high computational capabilities but also incorporate robust security features and support for emerging cryptographic standards. This study highlights the importance of understanding application-specific requirements and evaluating processor architectures accordingly. Future trends, including the rise of post-quantum cryptography and advancements in hardware acceleration, will influence processor design and selection, making it essential for system designers to stay informed and adaptable to ever increasing

References

[1] Jia Hao Kong, Li-Minn Ang, Kah Phooi Seng, “A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments”, Journal of Network and Computer Applications 49, 15–50, 2015.

[2] Jitendrakumar P. Radadiya, Dr. Haresh B. Tank, Journal of the Maharaja Sayajirao University of Baroda, ISSN : 0025-0422, Volume-55, No.1 (II) 2021.

[3] Bahram Rashidi,” A Survey on Hardware Implementations of Elliptic Curve Cryptosystems, arXiv:1710.08336v1,Oct 2017

[4] Pravin B. Ghewari, Mrs. Jaymala K. Patil, Amit B. Chougule, “Efficient Hardware Design and Implementation of AES Cryptosystem”, International Journal of Engineering Science and Technology Vol. 2(3), 213-219, 2010.

[5] Miguel Antonio Caraveo-Cacep, Rubén Vázquez-Medina, Antonio Hernández Zavala, “A survey on low-cost development boards for applying cryptography in IoT systems”, Internet of Things, Elsevier,Volume 22, 100743, ISSN 2542-6605, 2023.

[6] Luis Parrilla, Encarnación Castillo, Diego P. Morales and Antonio García , “Hardware Activation by Means of PUFs and Elliptic Curve Cryptography in Field-Programmable Devices”, MDPI, Electronics, 5, 5, 2016.

[7] Kazim Yumbul and Erkay Sava, “Enhancing an Embedded Processor Core for Efficient and Isolated Execution of Cryptographic Algorithms’, Section D: Security in Computer Systems and Networks, The Computer Journal, 2014.

[8] Shay Gueron, “Memory Encryption for General-Purpose Processors”, IEEE Computer and Reliability Societies, 1540-7993, 2016.

[9] Heeseung Jo, Seung-Tae Hong, Jae-Woo Chang, Dong Hoon Choi, “Data Encryption on GPU for High-Performance Database Systems”, Procedia Computer Science, Volume 19, Pages 147-154, ISSN 1877-0509, 2013.

[10] Brijgopal Bharadwaj, J. Saira Banu, M. Madiajagan, Muhammad Rukunuddin Ghalib, Oscar Castillo, Achyut Shankar, “GPU-Accelerated implementation of a genetically optimized image encryption algorithm”, Springer, Soft Computing, 25:14413–14428, 2021.

[11] Rajat Suvra Das, Vikas Gupta, “A Systematic Literature Review on Graphics Processing Unit Accelerated Realm of High-Performance Computing”, International Journal of Computing and Engineering ISSN 2958-7425, Vol. 5, Issue No. 3, pp. 10 - 21, 2024.

[12] Nabihah Ahmad, S.M.Rezaul Hasan, “A new ASIC implementation of an advanced encryption standard (AES) crypto-hardware accelerator”, Microelectronics Journal, Volume 117, 105255, November 2021.

[13] Ganesh T S, T S B Sudarshan, “ASIC Implementation of a Unified Hardware Architecture for Non-Key Based Cryptographic Hash Primitives”, International Conference on Information Technology: Coding and Computing, 0-7695-2315-3/05, IEEE.

[14] Shahwar Ali, A Humaria, M Sher Ramzan, Imran Khan, Syed M Saqlain, Anwar Ghani, J Zakia, and Bander A Alzahrani, “An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks”, International Journal of Distributed Sensor Networks, Volume 16, Issue 6, June 2020.

[15] Mahmoud A. Abdelaal , Abdellatif I. Moustafa , H. Kasban, H. Saleh, Hanaa A. Abdallah and Mohamed Yasin I. Afifi, “DNA-Inspired Lightweight Cryptographic Algorithm for Secure and Efficient Image Encryption”, IEEE Sensors,2322, 2025.

[16] Alexandru Coman, Radu Frățilă, “Cryptographic Applications using FPGA Technology”, Journal of Mobile, Embedded and Distributed Systems, vol. III, no. 1, ISSN 2067 – 4074, 2011.

[17] Jasvir Singh Kalsi, Jagpal Singh Ubhi, Kota Solomon Raju, "Design Advancements in Light-Weighted Symmetric Encryption for IoT applications on FPGA: Focusing on AES and DES Derivatives", International Journal of Engineering Trends and Technology, Volume 72, Issue 8, 292-311, ISSN: 2231–5381, August 2024.

[18] Yashar Salamia, Vahid Khajehvand, Esmaeil Zeinali, "Cryptographic Algorithms: A Review of the Literature, Weaknesses and Open Challenges", Journal of Computer & Robotics 16(2), Summer and Autumn 2023, 63-115.

[19] Fauziyah, Zhaoshun Wang, and Mujahid Tabassum, "A Holistic Secure Communication Mechanism Using a Multilayered Cryptographic Protocol to Enhanced Security", Computers, Materials & Continua, vol.78, no.3, 2024.