Review

JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)

Vol.31; No.1.| 2023

A Survey of Parallel Message Authentication and Hashing Methods

Yamamh Alaa[1*], Ahmed Fanfakh [2] and Esraa Hadi [3]

[1,2,3]College of Sciences for Women, University of Babylon, yamamah.alamari.gsci23@student.uobabylon.edu.iq, Hilla, Babel.

***Corresponding author email:** yamamah.alamari.gsci23@student.uobabylon.edu.iq; mobile: 07718469183

مصادقة الرسائل المتوازية والتجزئة

يمامه علاء[*1]، احمد بدري مسلم[2]، إسراء هادي[3]

[3,2,1] كلية العلوم للبنات ، جامعة بابل ، yamamah.alamari.gsci23@student.uobabylon.edu.iq، الحلة، بابل

Received:	15 /1 /2023	Accepted:	27 /3 /2023	Published:	31 /3 /2023

Abstract

Background:

Currently, there are approximately 4.95 billion people who use the Internet. This massive audience desires internet shopping, information exchange, social networking, and other activities that have grown dramatically in recent years. Therefore, it creates the need for greater confidentiality and privacy. In recent days, fraud via the Internet has been one of the key impediments to the dissemination of the use of business apps. Therefore, the three important security concerns actually occur daily in our world of transparent fashion, more accurately: identity, authentication, and authorization. Identification is a procedure that permits the recognition of an entity, which may be a person, a computer, or another asset such as a software programmer.

Materials and Methods:

In security systems, authentication and authorization are two complementary procedures for deciding who may access the information resources across a network. Many solutions have been presented in the literature. To get more performance on the authentication algorithmic, researchers used parallelism to increase the throughput of their algorithms. On the one hand, various approaches have been employed to enhance the security of cryptographic systems, including increasing the number of rounds, utilizing substitution tables, and integrating other security primitives for encryption and message authentication.

Results:

Recent studies on parallel message authentication and hashing algorithms have demonstrated that GPUs outperform other parallel platforms in terms of performance.

Conclusion:

This work presents a parallel implementation of message authentication techniques on several platforms. It is studying and demonstrating works which discuss authentication, hashing, and their implementation on a parallel platform as a main objective.

Key words:

Message Authentication, Hashing, cryptography, parallel computing

الخلاصة

مقدمة:

الإنترنت، وتبادل المعلومات، والتواصل الاجتماعي، وغيرها من الأنشطة التي ازدادت بشكل كبير في السنوات الأخيرة. لذلك، يتطلب الأمر زيادة السرية والخصوصية. في الأيام الأخيرة، كان الاحتيال عبر الإنترنت واحدًا من العوائق الرئيسية لنشر استخدام تطبيقات الأعمال. وبالتالي، تحدث الثلاث مخاوف الأمنية الهامة بشكل يومي في عالم الأزياء الشفافة لدينا، وهي: الهوية، والمصادقة، والترخيص. التعرف هو إجراء يسمح بتحديد هوية كيان ما، والذي يمكن أن يكون شخصًا أو جهاز كمبيوتر أو أصل آخر مثل مبرمج برامج.

طرق العمل:

في أنظمة الأمان، المصادقة والترخيص هما إجراءان مكملان لتحديد من يمكنه الوصول إلى موارد المعلومات عبر الشبكة. تم تقديم العديد من الحلول في الأدبيات. وللحصول على أداء أفضل في خوارزميات المصادقة، استخدم الباحثون التوازي لزيادة الإنتاجية لخوارزمياتهم. من جهة، تم استخدام مجموعة من الطرق لزيادة مستوى الأمان في الأنظمة التشفيرية، بما في ذلك زيادة عدد الجولات، واستخدام جداول الاستبدال ودمج آليات الأمان الأخرى لتشفير الرسائل والمصادقة عليها.

النتائج:

أظهرت الدراسات الحديثة حول مصادقة الرسائل المتوازية وخوارزميات التجزئة أن وحدات معالجة الرسومات تتفوق في الأداء على الأنظمة الأساسية المتوازية الأخرى من حيث الأداء.

الإستنتاجات:

يقدم هذا العمل تنفيذًا متوازيًا لتقنيات مصادقة الرسائل على العديد من الأنظمة الأساسية. تدرس وتعرض الأعمال التي تناقش المصادقة والتجزئة وتنفيذها على منصة موازية كهدف رئيسي.

الكلمات المفتاحية:

مصادقة الرسائل، التجزئة ، التشفير ، الحوسبة المتوازية

1-Introduction

Computer systems have grown rapidly during the last 20 years due to the development of networks, which have become vital tools in a variety of environments. Moreover, networks are indeed being developed by companies in greater proportions than ever before, and access to the global Internet has become essential. This pattern has been matched by an increase in unauthorized access to computer systems through the use of computer networks. Everyone knows that the Internet is a strong platform that transforms how we do business in today's technology. It now influences every facet of our lives, in addition to the emergence of more security-related dangers. We are prepared to begin this destructive journey [1] . In recent years, Internet use has grown at an accelerating rate and has become an integral aspect of daily life. It is believed that there are now more than 4.95 billion users of the internet worldwide [2] . Therefore, the appearance of the information security has significantly changed our lives, especially with the availability of information and the flexibility to view and modify the data. With the advent of Internet banking and electronic commercial exchanges, activities that were previously primarily conducted offline, like banking and market trades, are now primarily conducted online [1] .However, there is a need to secure all categories of resources and data from a variety of attacks aimed at numerous security services, including source authentication, integrity of data, and confidentiality of information. Cryptographic algorithms are frequently used to assure the security of these services. Existing attacks are divided into two types: active and passive. Active attacks may jeopardize data authenticity, integrity, and availability, while passive attacks can substantially endanger data confidentiality and user privacy. Furthermore, an active attacker has

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

the ability to insert, edit, or remove data content. Passive attacks are the sort of attacks in which the attacker reads or a copy of a message's content, jeopardizing their confidentiality [3] . The system is not affected as a result of the passive attack. The most critical aspect of a passive attack is that the victim is not notified of the attack, making it difficult to detect [4] . Figure[1] shows the relation between Active and passive attacks.

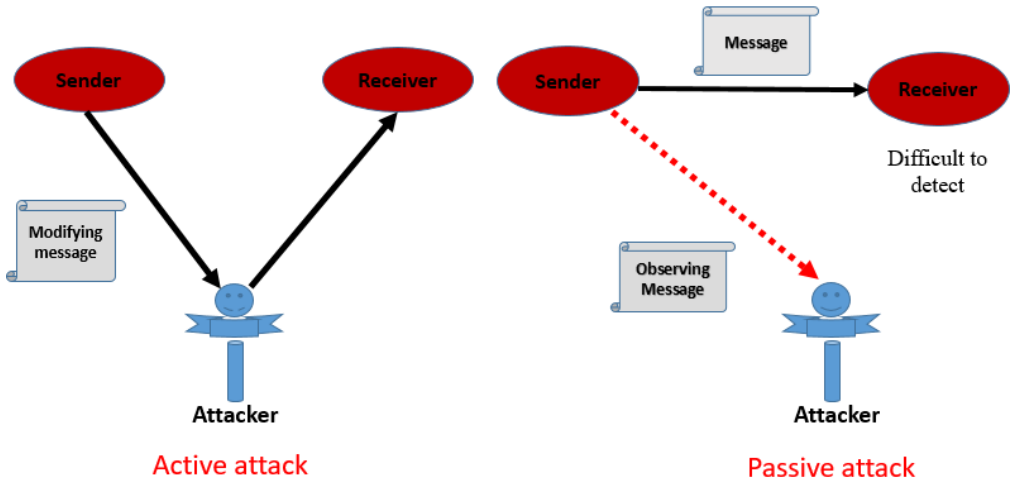


Figure (1): Active and passive attacks

Such assaults will cause significant harm. With the expansion of data and the Internet, it is necessary to protect all types of resources and data from all types of assaults by addressing security characteristics including data confidentiality, data integrity, and source authentication. Applying message authentication algorithms (MAA) helps overcome the challenges connected to message authentication assaults. A message authentication method's primary objective is to ensure that two (or more) parties with access to rrfffffffffthe same secret key can communicate and, most likely, recognize changes to the message while it is being transmitted. This stops an attacker from modifying the message to have undesirable effects. Additionally, block cipher-based or hash-based methods are used in typical symmetric message authentication procedures. [4] . The suggested approach entails breaking the message up into blocks, each of which has a unique dynamic key. The message authentication process is then implemented in parallel for each thread for the local MAC value, after which all threads interact with one another for the global MAC account.

2. Message Authentication Fundamentals

This section deals with basic definitions and principles before moving on to the many available approaches. Various entities are implied by the authentication process:

- In order to utilize the services, the claimant must authenticate with the system. It might be a person or an object.
- The "monitor" is the organization that offers an authentication service. It confirms (or denies) a claimant's identification. In the event of a failed authentication, it attempts to grant him/her access to the required service.
- If the monitor successfully validates them, the information system (IS) offers services like access to a computer account, an app, door unlocking, or a print server and will permit the client to utilize them (with a predetermined amount of trust).

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

A worker, for example, requires access to his or her workplace. An authentication system key protects the main entrance. If the token is given to the lock's token reader, it will release the door, regardless of whether the verification system thinks this worker is permitted to visit the building. The plaintiff is the worker in this case, the monitor is the verification system, and the IS's function is to open the main door [1] .

2.1 The Message Authentication Theory

In fact, the terms "identification," "authentication," and "certification" stand for three interconnected ideas that form the system's central component. An identification is the communication of an identity to an IS. Before utilizing the authentication, the claimed frequently gives the IS with an identification, and the monitor checks the identity via authentication. An authentication is evidence presented by a claimant to establish to a monitor that the person is that who they claimed to be. There are two questions must be addressed by authentication systems, the first one: who is the user? And the second: who he/she claims to be? Portrays himself/herself to be? As a result, authentication is among the most efficient strategies for establishing trust which can be used as an enhancement of security for business applications [1] .Figure 2 shows the keyed message authentication schema.

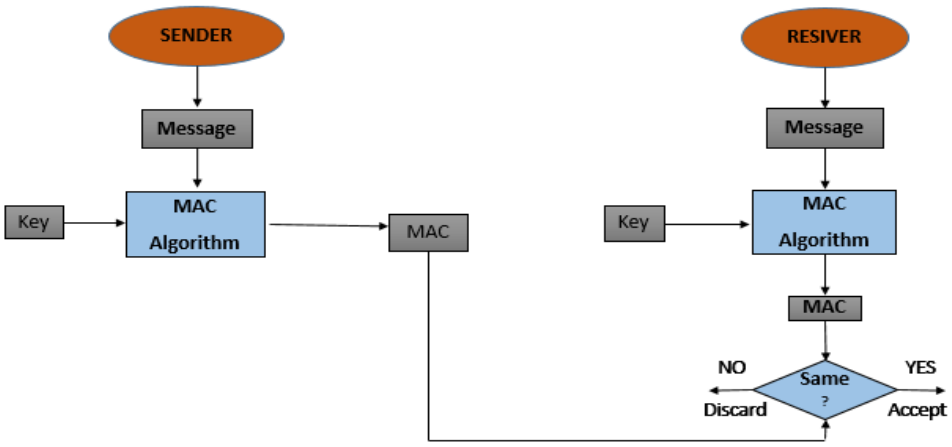


Figure (2): Message authentication schema

Then we need to connect the monitor and claimant. This link is known as a channel. A channel is a method of communication between the claimant and the monitor. It might be regarded as private, real, safe, or unsafe. A confidential channel resists eavesdropping, a genuine channel resists manipulation, a secure channel resists both, and an unsecure channel resist neither. The goal of authentication is to create a new identity, yet there is a wide variety of authentication techniques that might differ substantially. These authentication methods include USB tokens, smartcard PINs, image recognizers, and password identification [1] .

2.2 Hash function

Since quite some time, the phrase "hash function" has been used in computer science to describe a function that condenses a string of arbitrary input into a string of predetermined length. Nevertheless, if it complies with a few more conditions (which are described below), it may be utilized for cryptographic purposes and is then referred to as "cryptographic hash functions Authenticity, digital signatures, pseudo-number generation, digital steganography, digital time stamping, and other security objectives are all achieved using cryptographic hash functions, one of the most crucial tools in authenticity, digital signatures, pseudo-number generation, digital steganography, digital time stamping, and other security objectives are all achieved using cryptographic hash functions, one of the moshe field of cryptography. According to

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Gauravram's thesis, the use of cryptographic hash functions in a variety of information processing applications to meet different security objectives is far more common than the use of block ciphers and stream ciphers [5] .

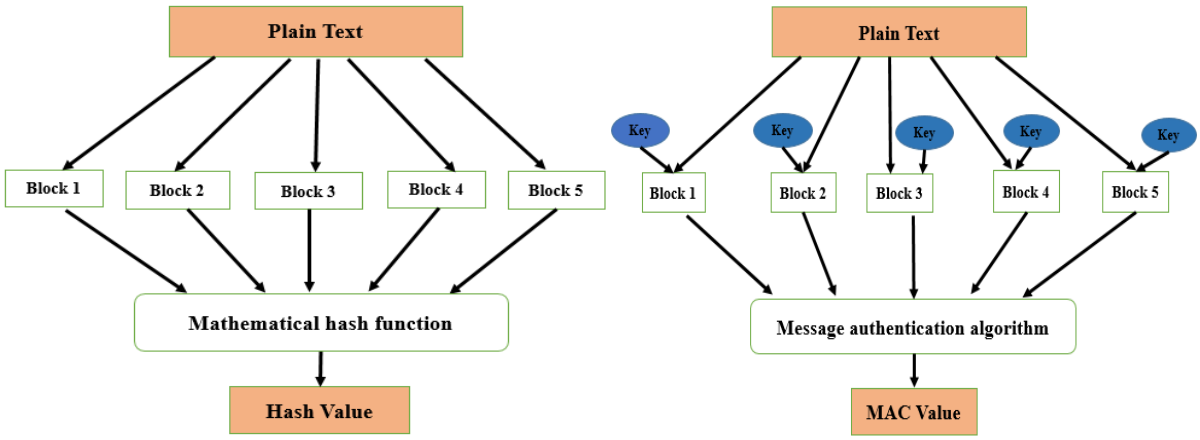
2.3 Comparing the message authentication and hash function

The hash function is a crucial piece of cryptographic equipment that is frequently combined with digital signature methods to ensure data integrity. The hash function accepts a message as input and produces a hash value, or just hash, as a result. In further detail, a hash function h converts bit strings of changeable finite size to strings with limited length. Figure 3 shows the main differences between a hash function and a MAC in term of Integrity, Authentication, Non- repudiation. These three terms can be defined as follows:

- Integrity: It is the absence of a flawed system or unauthorized data alterations.
- Authentication: it verifies the originality of the message for the recipient. The shared key between the sender and receiver is the proof of this verification process.
- Non-repudiation: It ensures the aforementioned characteristics as well as the sender's inability to deny responsibility for the communication [6] . Table 1 demonstrates the comparison between the hash and MAC.

Table 1: Comparison between Hash and MAC

Cryptographic primitive Security Goal	**Hash**	**MAC**
Integrity	yes	yes
Authentication	no	yes
Non-reputation	no	no
Key type	non	symmetric key



Figure[3] : Comparison between Hash and MAC

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

3. Review of parallel Authentication and hashing methods

As mentioned before, both MAC and Hash values confirm the message's integrity. Hash value is a non-key dependent strategy for certifying non-changing content but not for sending authentication. MAC values can be used for both of these issues. The performance of both hash and mac algorithms is improved by running them in parallel. Many researchers implement the hashing and authentication methods in parallel to get more throughput. The subsections that follow present some parallel works for both of these approaches.

3.1. Parallel hash functions

Secure-hash algorithms (SHAs), of which SHA-256 continues to be the most secure and effective, are essential elements of securing communication. Most signature algorithms, along with most quantum-resistant ones, employ SHA-256. The work in [7] proposed a parallel SHA-256 implementation for hashing hundreds of messages on the Sunway TaihuLight's SW26010 many-core processor, which is one of the world's fastest and most powerful computers. A common method for authenticated encryption is AES/GCM. Galois HASH (GHASH), which handles the authentication process, is one of its components. An effective mainframe-independent hardware design for parallel-pipelined GHASH was presented by researchers in [8] . The Galois Field (GF) multiplication algorithm is known as the Karatsuba-Ofman Algorithm (KOA). They used a single reduction array for all parallel KOA multipliers, unlike other parallel hardware architectures based on KOA. An area-optimized design has been accomplished as a consequence. In [9] , one of the primary methods for information security is the hash function, which serves as the basis for cryptography. Recently, there has been a lot of interest in the study of chaos-based hash functions. However, the related analysis is years behind. A unique, effective method for parallel hash functions based on a high-dimensional chaotic map was suggested in the paper. By using two nonlinear coupling constants, the suggested method significantly amplifies the diffusion impact as well as the confusion. Theoretical and empirical data demonstrate that the suggested system can satisfy all performance criteria for a hash function, including the need for desired statistical features and a sizable collision resistance. The suggested method has a high adoption potential for network security while also having the capacity to maintain parallel merit and message sensitivity. The recommended method is characterized primarily by a parallel processing mode and message extension in [10] . The algorithm continuously rounds the decimal fractions to integers before iterating the chaotic asymmetric tent map and chaotic piecewise linear map with parameters that can be changed based on the position index of the corresponding message blocks. Finally, the algorithm cascades these integer values to create an intermediate hash [10] .

3.2 Parallel message authentication function

Recent advancements in Graphic Processing Unit (GPU) technology have piqued the attention of researchers in applying and creating more efficient encryption techniques. Existing encryption technologies, such as AES and Secure Hash Functions 3 (SHA3), have been used to boost the performance of GPUs. The work in [4] developed a novel Message Authentication Algorithm (MAA) termed "DKEMA" is suggested in this work to better suit the GPU capability and idea. The proposed method is based on the dynamic key-dependent scheme and includes a single round of substitution and diffusion operations. Data security algorithms have to be implemented in order to safeguard personal and financial data due to the increased demand for online banking and personal data gathering on digital platforms. A brand-new authentication method known as Parallel Cipher-based Message Authentication Code (PCMAC) is put out in [11]. The suggested approach has a parallel design that makes it suitable for high-throughput applications. The suggested approach is conducted on an FPGA and compared to MAC-based authentication schemes. According to the testing results, the throughput of the PCMAC technique for authentication is 2.99 GB/s.Due to its extensive capacity and long data field length, the Controller Area Network utilizing Flexible Data-rate (CAN FD) is suitable for in-vehicle communication of the Internet of Related Vehicles

(IoCVs).However, CAN-FD is extremely susceptible to masquerade attacks since it lacks a security authentication mechanism. A two-stage technique for enhancing security for a real-time parallel in-vehicle application was provided in the work in [12] .The majority of sequences are swiftly removed in the first step in order to establish the lowest restriction for an in-vehicle application. In the second step, security is improved by including Message Authentication Codes (MACs) in communications between the lower bound and the deadline.

4. Comparative analysis

The foundation of conventional authentication is the usage of a password file, which keeps track of both user IDs and hashes of the passwords associated with each user. Upon logging in, a user's password is hashed and compared to the value stored in the password file. The user is authorized if the two hashes coincide. In order to extract passwords from hashed passwords, for instance, attackers who get access to a system's password file may employ brute-force attacks. Additionally, this method can require repeated authentication for existing programs that access resources across many platforms. It may be possible to somewhat decrease the problems associated with password-based authentication by utilizing more clever passwords and login names that adhere to requirements like minimum length and complexity, including capital letters and symbols. On the other hand, systems that need several independent forms of authentication are more susceptible than those that rely just on passwords and expertise. The following other authentication techniques have been used:

- Authentication using two-factor authentication requires users to enter a second authentication factor in addition to their password, adding an extra degree of security to the procedure. Users of 2FA systems frequently have to enter a verification code generated by an authentication program, transmitted through text message to a mobile phone or other preregistered device, or a code they received via text message.
- MFA requires customers to employ several forms of authentication, such as a possession factor (like a security key fob), a biometric factor (like a thumbprint or face recognition), or a token produced by an authenticator app.
-OTP: An OTP is a string of letters and numbers that is produced mechanically to verify a user. This password, which is only valid for one login process or transaction, is frequently used by new users or users who have forgotten their passwords and were provided with an OTP to log in and reset their password.
-Using three factors for authentication entails combining a learning element, such as a password, with a possession element, such as a security token, and an inherent factor, such as a biometric.
- Biometrics are often employed as a second or third authentication component, while certain authentication systems are completely dependent on biometric identity. The most common biometric identification technologies are fingerprint scanning and facial recognition. as well as retinal scans and speech recognition [13] . Table 2: Comparative Research of Authentication Methods is followed by Table 3, which compares all of the previously described parallel authentication strategies in this study.

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Table 2: Comparative study between well-known authentication methods

Method	Security level	Key type	Ease of use	cost
2FA	**	**Symmetric key**	****	***
MFA	***	**Asymmetric key**	******	**
OTP	****	**Symmetric key**	***	****
Three factors	*****	**Asymmetric key**	*****	**
Biometric	******	**Symmetric key**	***	**

The security level is as important as the computational cost of the authentication algorithm. Many researchers, however, used the authentication algorithm to obtain the MAC value faster by applying them algorithm on parallel. Thus, table (3) demonstrates the comparison between the existing parallel authentication methods. The table uses star symbol to represent the level of each factor, more stars is the best. Several metrics which concern parallelism and security are taken into consideration in the comparison.

- Parallel platform: It is the architecture used, such as CPU, GPU, multi-core, and others.
- Length of key: The length of the key affects most algorithms' complexity in terms of the number of rounds.
- Type of key: If the key is symmetrical, it is easier to apply in parallel compared to an asymmetrical key method.
- Number of rounds: normally is used is to increase the level of security, which mostly depends on the length of the key.
- Security level: Depends on the length of the key and the number of rounds.
- Throughput is the number of information units (message size) that a system can process in a given amount of time.

To evaluate each method that mention in the comparison table 3, the best one can give more security level when the key size is increased, while producing higher throughput.

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

Table 3: comparison between the parallel authentication methods

Ref	description	Parallel platform	Length of key	Type of key	Number of rounds	Security level	Throughput
[4]	They demonstrated a method that was more suitable for GPU capacity and concept. The dynamic key-dependent system, which includes one round of substitution and diffusion methods, is the foundation of this system.	GPU	128,192 ,256 bits	Symmetric Dynamic key	1 round	high level of perform ance and security	more than 400GB/s
[7]	They provide SW-SHA-256 as a parallel SHA-256 solution for hashing numerous messages on the SW26010 many-core processor of the Sunway TaihuLight	Many-core CPU	256	Symmetric static key	16 rounds	high	7.29 GB/s on a single SW26010 process
[8]	They describe an effective Karatsuba Ofman Algorithm (KOA) based Galois Field (GF) multiplication hardware implementation for parallel-pipelined GHASH.	Multicore CPU	_	_	_	high	113.8 GB/s
[11]	They have introduced parallel cipher-based message authentication code, a novel authentication technique (PCMAC). The suggested technique has a parallel design and is effective for applications requiring high throughput.	Multicore CPU	128 bits	Symmetric key	_	high	2.99 GB/s
[14]	For serial modes, they offered a brand-new, simple implementation method. It focuses more on serial MAC (authentication) and AE modes, where each input block must be processed sequentially in accordance with the original specifications.	multicore CPU	128 bits	Symmetric key	_	large security	_

1992-0652 ISSN
abylon.com
p@itnet.uobabylon.edu.i
info@

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

5. Conclusion

In this paper, a parallel implementation of message authentication methods across different architectures is presented. The aim is to study and demonstrate papers that deal with authentication and hashing and their implementation on a parallel platform. The results of all works are presented in terms of platform type, key length and type, number of rounds, level of security, and throughput. The primary goal of the parallel computing researchers is to improve the throughput of the authentication algorithms used. This study also noticed that most of the methods that depend on the symmetric key are easier to program in parallel compared to the ones that use the asymmetric key.

6. Acknowledgments

Researcher would like to thanks university of Babylon / College of Sciences for Women for supporting this work.

Conflict of interests.

There are non-conflicts of interest.

References

[1] S. Zulkarnain, S. Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, "A Review on Authentication Methods," *Aust. J. Basic Appl. Sci.*, vol. 7, no. 5, pp. 95–107, 2013, [Online]. Available: https://hal.archives-ouvertes.fr/hal-00912435%0Ahttps://hal.archives-ouvertes.fr/hal-00912435/document

[2] A. Roberts, S. Sharman, and H. Bowden-Jones, "Clinical services for problematic internet usage," *Curr. Opin. Behav. Sci.*, vol. 46, no. July, p. 101180, 2022, doi: 10.1016/j.cobeha.2022.101180.

[3] A. Fanfakh, H. Noura, and R. Couturier, "ORSCA-GPU: one round stream cipher algorithm for GPU implementation," *J. Supercomput.*, vol. 78, no. 9, pp. 11744–11767, 2022, doi: 10.1007/s11227-022-04335-4.

[4] H. N. Noura, R. Couturier, O. Salman, and K. Mazouzi, "DKEMA: GPU-based and dynamic key-dependent efficient message authentication algorithm," *J. Supercomput.*, vol. 78, no. 12, pp. 14034–14071, 2022, doi: 10.1007/s11227-022-04433-3.

[5] R. Sobti and G. Geetha, "Cryptographic Hash Functions: A Review," *Int. J. Comput. Sci. Issues*, vol. 9, no. 2, pp. 461–479, 2012.

[6] M. A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen, "Efficient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad-Hoc Network," *IEEE Access*, vol. 7, pp. 71424–71435, 2019, doi: 10.1109/ACCESS.2019.2919973.

[7] Z. Wang, X. Dong, Y. Kang, and H. Chen, "Parallel SHA-256 on SW26010 many-core processor for hashing of multiple messages," *J. Supercomput.*, vol. 79, no. 2, pp. 2332–2355, 2023, doi: 10.1007/s11227-022-04750-7.

[8] K. M. Abdellatif, R. Chotin-Avot, and H. Mehrez, "Efficient parallel-pipelined GHASH for message authentication," *2012 Int. Conf. Reconfigurable Comput. FPGAs, ReConFig 2012*, no. 1, pp. 1–4, 2012, doi: 10.1109/ReConFig.2012.6416742.

[9] A. Akhavan, A. Samsudin, and A. Akhshani, "A novel parallel hash function based on 3D chaotic map," *EURASIP J. Adv. Signal Process.*, vol. 2013, no. 1, pp. 1–12, 2013, doi: 10.1186/1687-6180-2013-126.

[10] Y. Li, D. Xiao, S. Deng, Q. Han, and G. Zhou, "Parallel Hash function construction based on chaotic maps with changeable parameters," *Neural Comput. Appl.*, vol. 20, no. 8, pp. 1305–1312, 2011, doi: 10.1007/s00521-011-0543-4.

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

[11] S. J. H. Pirzada, A. Murtaza, J. Liu, and T. Xu, "The parallel CMAC authentication Algorithm," *2019 IEEE 11th Int. Conf. Commun. Softw. Networks, ICCSN 2019*, pp. 800–804, 2019, doi: 10.1109/ICCSN.2019.8905326.

[12] R. Xie, G., Yang, L. T., Wu, W., Zeng, K., Xiao, X., & Li, "Security enhancement for real-time parallel in-vehicle applications by CAN FD message authentication," *IEEE Trans. Intell. Transp. Syst.*, 2020.

[13] H. Zahid and U. Khan, "Comparative Study of Authentication Techniques," *Int. J. Video& Image Process. Netw. Secur. IJVIPNS-IJENS*, vol. 10, no. 04, pp. 103304–2929, 2010.

[14] K. Minematsu, A. Inoue, K. Moriwaki, M. Shigeri, and H. Kubo, "Parallel Verification of Serial MAC and AE Modes," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 13203 LNCS, pp. 200–219, 2022, doi: 10.1007/978-3-030-99277-4_10.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652