Authentication and Encryption of IoT Devices Based on Elliptic Curves: A survey

Ali E. Takieldeen[1], and Fahmi Khalifa [2]
[1]Faculty of Engineering, Hours University, Damietta, Egypt
[2]Electronics and Communications Engineering Department, Faculty of Engineering, Mansoura University
Mansoura Dakahlyis 35516, Egypt
Email address: a_takieldeen@yahoo.com, fahmikhalifa@mans.edu.eg

Abstract

With the progressive development of a wide range of applications that interconnect things, internet of things (IoT) become an imperative required trend by industries and academicians. IoT allows these things to be remotely accessed or controlled depending on internet protocol (IP) networks. This technology increases accuracy and efficiency of the tasks relied on, also facilitate daily people life. The huge applications domain infrastructure which depends on IoT, requires a trusted connection to guarantee a security and privacy while transferring data. IoT Privacy insurance essentially encounter many challenges to apply effective authentication protocols and procedures due to heterogeneous and dynamic nature. A lot of researches and theses have offered multiple ways for data authentication schemes depending on the underlying system architecture and a treatment to the security breaching problem caused by flaws and weak points in previous schemes. This paper provides complete and up-to-date review of lightweight cryptography for IoT authentication based on elliptic curve cryptography (ECC). ECC has many advantages if compared with other cryptographic systems. It is ideal to be implemented in most IoT devices specially in resource constrained devices with optimum implementation. That has been accomplished through delving into schemes with detailed explanation to guide future researchers in IoT lightweight authentication field. Furthermore, a comparison was performed with the proposals presented in the study to identify the considerations to design lightweight ECC scheme..

Keywords: Cryptography, Elliptic Curve, Internet of Things, Authentication, and Security analysis

1. Introduction

In recent years, remote access technology and device control has become an imperative requirement, which is evident nowadays through the increasing spread in the Corona pandemic (COVID-19), which necessitated the imposition of some restrictions, including the mandatory social distancing in many countries. Therefore, it became clear how developing remote access communication technology is the importance depending on the Internet service, especially researches in improving the technology of the Internet of things (IoT). Internet of things is the technology to assemble devices which needs to be monitored, linked and interacted [1]. IoT is associated with great prospects of physical objects with the cyber world such as healthcare devices, intelligent transportation system, home appliance, sensors and environmental monitoring [2]. Connected devices to IoT are exponentially increases [3] which added security challenges that must be taken into consideration [4]. As a result of huge amount of heterogeneous devices

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

coexisting in the market, that creates an open challenge as multiple technologies become existing in each layer of IoT architecture [5]. Figure 1 illustrates the basic structure of IoT [6] system architecture.

Despite the increasing number of users of IoT technology, many people are still concerned about the use of these technologies due to the security challenges which need at least the same security precautions of a conventional network that we will discuss through this research. Therefore, there is an urgent need to provide reliable communication services such as major distribution and object authentication systems [7,8].

The purpose of tis paper is provide an overview of the recent research for the authentication and encryption of IoT devices using Elliptic Curves. The reminder of this paper is sectioned as follows. In the next section, the methodology of this work is presented. A general introduction on cryptographic for IoT systems and litreature types is discussed in Section 3. The litreature cryptosystems up to August 2020 are summarized in Section 4 and Section 5 clarify difference and compare results of IoT authentication schemes. Finally, Section 6 presents a brief discussion about what was concluded in this work

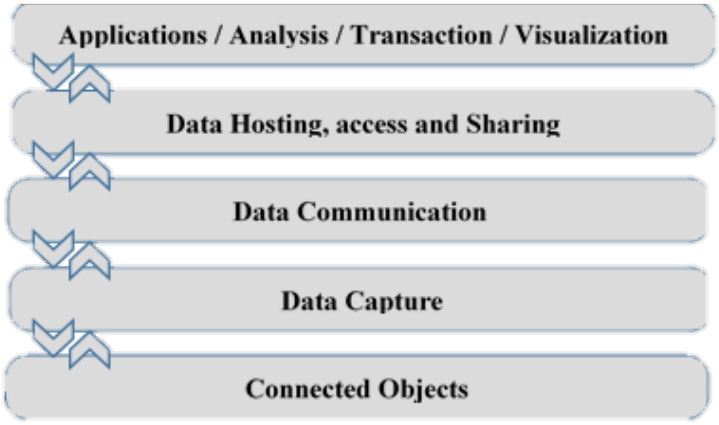


Figure 1– Blockdiagram for an IoT-based system architecture

2. Methodology

This survey was a search process of the research revolving around keywords (lightweight, authentication, elliptic curve cryptography, ECC, Public key) through academic search engines and publishing corporations such as ScienceDirect, Hindawi, MDPI, IEEEXplore, Wiley, ACM Digital Library, springer and Elsevier. We can conclude the authors' motivations to these keywords in the robustness of algorithm, optimum implementation with the lowest cost, low power consumption. Selected papers were identified according to its contribution, design goals and the analysis of the reached results. Many papers did not include analytical description of its experimental results so they were discarded from the survey.

3. Cryptography for IoT Systems

Basically, there are three fundamental security issues: integrity, confidentiality and availability. Over time, several security requirements properties like authenticity, authorization, reliability, privacy, accountability, and physical security was required to be considered. Table 1 demonstrate a brief description has presented for authentication properties in IoT perimeter [9-13]. According to table 1, it is imperative to reduce security risks by permitting only authenticated and authorized users. Security services can be implemented using the traditional cryptography but it affects system's performance and efficiency. In addition to, obvious drawbacks in the Internet of Things (IoT) have been identified as insufficient confidentiality, lack of transport encryption, and less physical layer security [14]. That pushed towards thinking in what is currently called lightweight cryptography to overcome the flaws

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

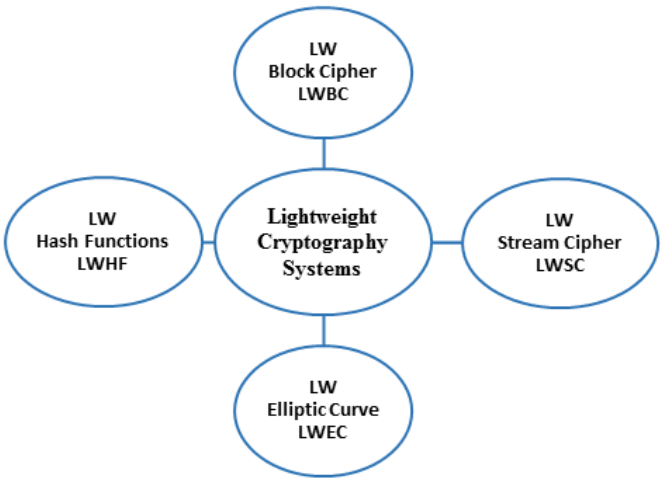
that appeared in traditional cryptography [15]. Lightweight cryptography is based on low cost cryptographic algorithms with low cost services that offers optimum size, performance, and security [16].

3.1 Lightweight cryptography

Block cipher cryptosystem, and hash functions as illustrated in figure 2 are both authentication schemes which is widely used in wireless networks [17,18]. Elliptic curve cryptography is also one of authentication schemes available in wireless communications to ensure the implementation of the encryption processes necessary to achieve required authentication [20]. A lot of researches in different application domains rely on the elliptical curve as a credibility scheme, which proved its strength when analyzing the results when subjected to many types of cyber-attacks [19-25].

Table 1: IoT authentication required properties [2,9,16]

Property	Description
Confidentiality	Ensures that confidential data transmission process is secured and not disclosed specially from connected devices to IoT system.
Authenticity	Enabling IoT devices to authenticate the peer by proof of identity to receive or transmit any information
Integrity	The safeguarding of previous generated data such as keys, medical record, credit card numbers, and billing logs which should retaining at a data warehouse
Availability	Ensuring the accessibility to IoT device or system upon required which can be affected by accidental or deliberate
Authorization	Determining the privilege of the connected parties to ensure if it is authorized to access a resource.
Non-repudiation (NR)	Ensure undeniable of messages between two objects in IoT system by archiving it in a trusted third party
Anonymity	Ensures that authorized party data cannot be accessed by intruders
Accountability	A property of tracking data transmission whether from a device or user
Attack resistance	is the property that ensures protection to authentication processes against attacks by using the authentication feature



DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

Figure 2– lightweight cryptography systems.

3.2 Security threats in the IoT

There is a progressive increase in security threats in correspondence to the large increase in the unprotected devices related to the Internet of things(IoT), which represents escalating threat to data privacy and devices in the network. An important reason, according to the report issued in [26], is the reliance on operating systems that are not approved and no longer have security support that contributes to achieving the necessary security and privacy from cyber-attacks. Figure 3 shows top IoT threats that targets IoT devices.

Table 2 presents number of threats that are applied in IoT systems with a brief description to each. These threats are depending on IoT layers whether it is application, network, software or physical layer. These descriptions are the summary for the researches [9, 27-29] that presents threats of IoT networks.

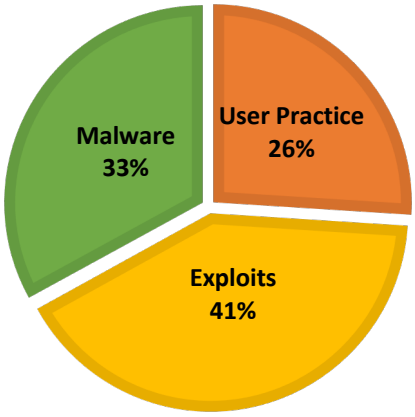


Figure 3– Top IoT threats, adopted from [26].

Table 2–Threat models in the IoT

Threat	Description
Denial of service attack	Attacker makes legitimate users are unavailable to use their resources by sending a torrent of legitimate-like requests which causes service to be stopped
Eavesdropping attack	The attacker eavesdrops on the existing communication between two parties over the network without interfering or changing that data, but its privacy is compromised also that enables the intruder to carry out attacks using that information
Impersonation attack	In this type of attack, the intruder exploits the previous type of attacks, by eavesdropping on two parties connection to gather information, then it is exploited to impersonate a legal user and act as a legal server
Password change attack	The attacker will carry out a chain of iterative operations, trying a large number of passwords until the successful change.
Stolen smart (verified) device attack	This attack depends on stolen pre-verified device by retrieving all stored information by applying power analysis attack
Sinkhole Attack	A malicious node takes over a node in the network by broadcasts delusory information about routings to trick specific nodes to make route through it then attract all information in addition to forward, modification or deleting these packets

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

Man-in-the-Middle Attack	Here not only, intruder eavesdrops the connection and stole sensitive information but also tries to make changes on the messages or delete it.
Side-channel Attacks	Here the attacker does not rely on the encrypted text or the original message, but rather relies on information that he captured from the side channel, trying to detect the encryption key through it. It could error frequency, energy, time required to perform the operation.

3.3 Lightweight stream cipher (LWSC)

Stream cipher is an encryption mechanism that encrypt and decrypt one bit at a time. There are many stream cipher algorithms as RC4 and E0 in addition to A5/1, Rabbit, Grain, and Trivium which was the first cryptographic mechanism used in lightweight stream ciphers (LWSC) [30]. A5/1, Rabbit, Trivium and Grain were one of the winner algorithms in project eSTREAM organized by EU ECRYPT network [31]. RC4 is a stream cipher algorithm which is widely included in software stream ciphers like Transport Layer Security (TLS), Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). It has many vulnerabilities, although it is not completely penetrated [32]. It is not preferred to be used in new applications. It's ciphersuite used in SSL/TLS is broken [33]. E0 is a stream cipher which is used in Bluetooth. It is the based stream cipher used in linear feedback shift registers (LFSR). Which has no immunity against cryptanalysis as Berlekamp-Massey algorithm [34]. Accordingly, all ciphers depend on LFSR vulnerable to various cryptanalysis techniques [31]. A5/1 is famous lightweight stream as an encryption algorithm used in GSM cellular security systems [35]. Many cryptanalysis attack succeeded to break the cipher within a few minutes based on time–memory tradeoff and other known-plaintext attacks [36].

3.4 Lightweight block cipher (LBSC)

According to [37] lightweight block ciphers are more suitable for low-resources devices with reasonable and acceptable security level. Block cipher algorithm depends on three main steps Encryption, decryption and key schedule. The operations are performed with fixed key length. it depends on iterative processes called rounds which make it easier to reach the desired robustness [38]. Figure 4 shows different types of LW Block Cipher.

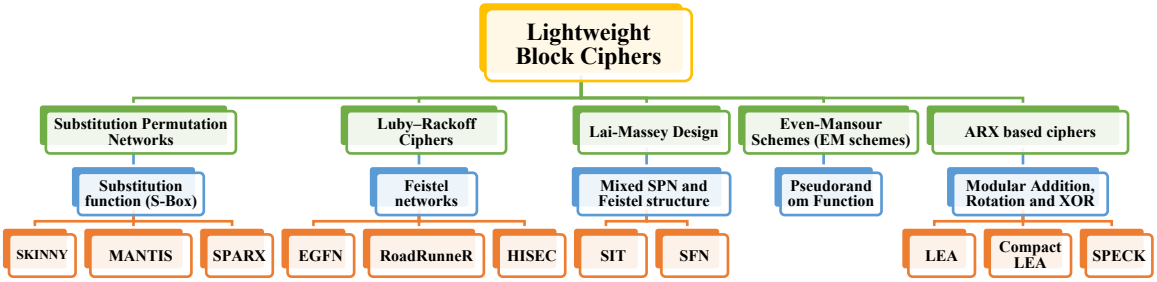


Figure 4– Lightweight block cipher (LWBSC) with techniques and algorithms [38-39].

3.5 Lightweight hash function (LWHF)

Hash function is the main step or algorithm to perform blockchain technology. Hash function don't have any improper performance if applied in resource-constrained devices with insufficient memory, power and area. Cryptocurrency is the basic function of hash function authentication at applications of blockchain [40,41]. Top lightweight hash functions have been summarized in Figure 4 in addition to blockchain-based coins.

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

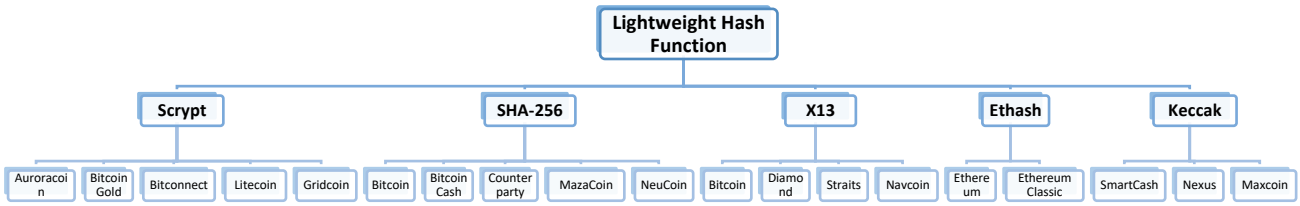


Figure 4– Lightweight hash functions with blockchain-based coins [41].

4. Surveyed Researches

Most of works related to the IoT has been studied from many aspects, as it is considered a nascent field in need of further research and study. One of the most important and wide issue studied was data authentication, security and privacy. The attention of many researchers relied on propose new schemes that supports lightweight security and authentication mechanisms. Most of studies methodologies are improving processing time and required storage area. In Table 3 a review of 2019 and 2020 studies in lightweight authentication schemes refined according to security analysis and Performance analysis. All works depends on protocols based on asymmetric lightweight scheme Elliptic curve.

Table 3–Summary from 2019 to 2020 for characteristics of the surveyed lightweight Elliptic Curve based protocols

Work	Basis	Participants	Security Analysis	Performance Analysis
Naeem et al. [4]	- ECC	- RFID Tag - RFID Reader	- Mutual authentication - Confidentiality, Anonymity - Forward security - Location privacy - Man-in-the-middle attack prevention - Prevention of replay attack - Impersonation Attack Avoidance - BAN LOGIC tool for authentication Proof	- Operation count - Computation Cost
Alamr et al. [22]	- ECDH - ECC	- RFID	- - Mutual Authentication - Anonymity - Confidentiality - Forward Security - Location Privacy - Man-in-the-middle attack - Replay attack - Impersonation attack	- Number of operations - computing time - storage cost

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

Nikooghadam et al. [27]	- ECC - Hash Function	- Servers. - IoT	- Insider attack. - Known-session-specific temporary information attack. - User impersonation attack - Server impersonation attack - Replay attack - Offline password guessing attack - Known-key secrecy - Denning-Sacco attack - Mutual authentication - Denial of service attack - Perfect forward secrecy	- Computation cost - Communication cost
Kumar et al. [42]	- ECC	- RFID Tag, - RFID Reader, - Sensor Node.		- Throughput, - jitter QoS.
S. Adhikari and S. Ray [43]	- Hash function - ECC	- Server. - Two party Auth.	- - Replay Attack Resilience, - - Man-in-the-Middle Attack Resilience - - Perfect Forward Secrecy - Known Session Key Attack Resilience - Brute Force Attack Resilience	
Jiang et al. [44]	- Hash Function - Chinese Remainder Theory - ECC - ECDH	- Smart homes	- Replay Attack - man-in-the-middle Attack - Security of the key agreement combination	- Computation overhead - Time consumption - Computational costs
Noori et al. [45]	- Hash Function - ECC	- RFID Tag - RFID Reader	- man-in-the-middle Attack - Forging Attack - insider attack - Mutual authentication - Forwards security - Replay attack - Masquerade attack	- Computation costs - Running time of the EC point multiplication

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

Shafiq et al. [46]	- Hash Function - ECC	- Two party	- Smart Card Stolen Attack - Password Guessing Attack - Replay Attack - Perfect Forward Secrecy - Mutual Authentication - Server and User Impersonation Attack - User's Privacy and Anonymity - Stolen Verifier and Insider Attack	- Computation cost - Storage cost - Communication cost
Y. S. Wei and J. h. Chen [47]	- ECC	- RFID Tag - RFID Reader NFC	- Tracking attack - DoS attack - Forward security - Spoofing attack - Replay attack - Mobile environment - Anonymity - Mutual authentication	-
Qin et al. [48]	- Key-policy attribute-based encryption - ECC - Elliptic Curve Qu Vanstone (ECQV) - Hash function	- Vehicular network	- Data Confidentiality - Conditional Anonymity - Mutual Authentication	- Execution time of access phase - time comparison of the encryption/ decryption process - Execution time of - Authentication operations - Communication costs of encryption and decryption phase
J. Guruprakash and S. Koppu [49]	- Hash function - ECC - Lightweight Scalable Blockchain (LSB) - EC-ElGamal	- IoT Blockchain		- Transaction Flow - Processing time - Hash quality - Hash Operation - Storage cost - Block Validation
Thungon et al. [50]	- ECDH - MAC ID	- 6LoWPAN	- Security verification tool (AVISPA) - BAN logic tool - AVISPA tool - Replay Attack - Man-in-the-middle Attack - Node compromised Attack - Node Tampering Attack - Sybil Attack - Compromised attack	- Computation overhead - Communication overhead

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

A. Aziz and K. Singh [51]	- ECC - Chaotic maps	- IoT	- The Oblivious Attacker - The Non-oblivious Attacker	-
A. Kumar and A. K. Jain [52]	- Hash Function - ECC	- RFID Tag	- Mutual Authentication - Forward Security - Tracking attack - Cloning attack	-
Khan et al. [53]	- Hash Function - Substitution-Ceaser cipher - Improved ECC	- Medical Sensors		- Hash function - Cost - Encryption/Decryption Time - Correlation coefficient
P. K. Panda and S. Chattopadhyay [54]	- ECC - Hash Function	- IoT - Cloud Servers	- Mutual authentication - Replay attack - Password guessing attack - Device privacy - Insider attack - Man-in-the-middle attack - Impersonation attack - Many logged-in device's attack - Session key agreement - Perfect forward secrecy	- Computational overhead - Communication overhead - Storage overhead - Computational time
P. G. Chilveri and M. S. Nagmode [55]	- ECC - Hash Function	- IoT. - MANET - WSN	- Mutual authentication - Session key agreement - User anonymity - Un-traceability - Freely password change - Replay attack - Stolen smart card attack - Session-specific temporary information attack - User impersonation attack - GWN impersonation attack - Sensor node impersonation attack - Avoid of clock synchronization problem - Reflected attacks - Server compromise	- Computational cost - Communication costs - Correlation analysis

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

S.Chatterjee and S. G. Samaddar [56]	- - ECC	- IoT - User's smart device - Cloud	- Confidentiality - Man-in-the-Middle Attack - Replay Attack - Perfect Forward Security - Session Key Attack	- Computational Cost
Alzahrani et al. [57]	- ECC - self certified keys	- IoT - Device 2 Device Auth.	- Key compromise impersonation attack - Device Anonymity - Man in Middle Attack; - Known Key attack - Unknown Key Share Attack - Perfect Forward Secrecy Known - Session Specific Information Attack - Key Offset/Replicate Attack - No Key Control - Replay Attack	- Communication Cost - Computational Cost
Sowjanya et al. [58]	- - ECC (point multiplication) - - Hash Function - -	- - Healthcare (WBAN)	- Perfect forward secrecy - DoS attack - No key control - Clock synchronization - User anonymity - Impersonation attack - Known Session-specific Temporary Information (KSSTI) attack - Insider attack - Key security - Non-traceability - Mutual authentication - Modification attack - Replay attack - Man-in-the-middle attack - Stolen verifier table attack	- - Security features comparison - - Storage cost comparison - - cost comparison - - Communication cost
Z. Xie and L. Jiang [59]	- ECC - Hash Function	- -IoT	-	- Computation overhead - Communication cost - Storage cost

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

Gyamfi et al. [60]	- ECC	- - Mobile Environment	- Mutual Authentication and Session Key Exchange - Anonymity - Replay Attacks - Impersonation Attacks - Forward Secrecy - Man-in-the-middle Attacks - Password Change Attacks - Privileged Insider Attacks - password change facility	- Computational Overhead - Communicational Overhead
Nino et al. [61]	- ECC (binary Edward curves)	- IoT		- Throughput - Throughput per gate equivalent (GE) - Throughput per slice (SLC)
Kasyoka et al. [62]	- Hash function - ECC	- WSN	- Compromise attack. - replay attack - Denial-of-service attack - User anonymity - Mutual authenticity - Man-in-the-middle attack	- Computational cost - Communication cost - Computational energy cost - Broadcast authentication time
Das et al. [63]	- ECC - Hash function	- IoT	- replay attack. - malicious device deployment attack - man-in the- middle attack - Device physical capture attack - Device impersonation attack. - Ephemeral Secret Leakage (ESL) attack. - Mutual authentication - formal security analysis	- communication costs. - computation costs. - end-to-end delay. - packet loss rate. - Throughput.
Seok et al. [64]	- ECDSA-Sign - ECDSA-Verify - ECDH - AEAD	- IoT (device 2 device)	- Impersonation attack. - Eavesdropping - Privacy sniffing. - Free riding attack and location spoofing	- - Area - - Power - - Throughput - - Energy
ZHOU et al. [65]	- ECC (NIST / SM2)	- IoT		- Cycle Counts of Finite Field Arithmetic Software - Cycle Counts and Code Size of Scalar Multiplication - Software. - AVR - ATmega128Microcontrollers

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

Although, also symmetric schemes have low computational complexity, the protocol layer requires time synchronization between devices and a significant amount of overhead for communication and storage [66]. Ii is a challenging task to put the rules of design scheme that possess knowledge of cryptographic and authentication basis resist most of attacks. Elliptic curves have an impressing factor in choosing it as an encryption and authentication with lightweight nature. ECC has special curves shown in figure 5. These curves provide efficient computation and performance. Many researchers used these types of curves such as [24] who used Montgomery and twisted Edwards curves in his software. While [65, 68] used have used basic form of Elliptic curve or Weierstrass curves over prime fields.

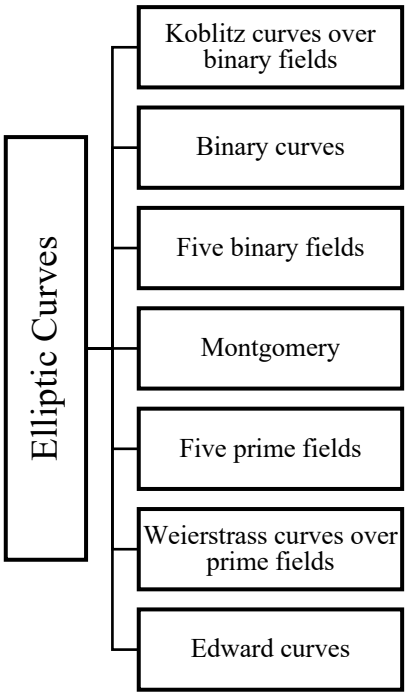


Figure 5– Special Elliptic Curves [67].

5. Review of The Litreature Results

In this section, results of some researches were presented depending on its performance analysis. Table 4, illustrate each research publication year, and the vast majority of it was in 2020, which is what we intended in order to be an index for researchers to know the latest researches with its performance results related to the lightweight authentication based on the elliptical curve as its basic cryptography algorithm. The three main factors that were clarified for the results in the table were the cost of communication, computation, and storage. There may be some research that did not clarify one of these costs, so it was not included.

Work	**Performance analysis**				
	Computational Cost	**Communication Cost**	**Storage Cost**	**Energy**	**Correlation C.**

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

Naeem et al. [4], 2019	Tag: $3T_m + T_a + 2T_h \approx 6.7114$ ms Reader: $3T_m + T_a + 2T_h \approx 6.7114$ ms T_m: point multiplication execution time T_a: point addition execution time T_h: one-way hash function execution time	512 bits / 3 MSG	-	-	-
Nikooghadam et al. [27], 2019	User: $3T_{mu}+T_{hf}+2T_{en/d}+2T_{ad}$ Server: $T_{mu}+2T_{hf}+4T_{en/d}+2T_{ad}$ Total: $4T_{mu}+3T_{hf}+6T_{en/d}+4T_{ad} \approx 30.2306$ ms T_{mu}: scalar multiplication time = 7.3529 ms T_{hf} : Hash function operations time = 0.0004 ms $T_{en/d}$: Symmetric encryption operations time = 0.1303 ms T_{ad}: Two point addition operations time = 0.009 ms	1280 bits/ 3 Msg	-	-	-
Jiang et al. [44], 2020	$4\ T_m + 4\ T_h$ T_m: Scalar multiplication time T_h: Hash function time	Total memory cost on the sensor node side: 2265 bits. Total memory cost on the central server node side: 1978 bits.	-	-	-
Shafiq et al. [46], 2020	$4Tm+9Th + 8T_{\oplus} + 17T_{\|\|} \approx 0.00985$ ms Th: time for calculating hash function. Tm: time for calculating the dot	Cost of Registration: 928 bits Cost of login and authentication:	672 bits	-	

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

Thungon et al. [50], 2020	Gateway node: $8T_h$ Sensor node:$6T_h$ User: - Server: 4 T_h Total: 18 T_h T_h: time for calculating hash function.	-	-	-	-
Khan et al. [53], 2020	User: 4H + Ec + Dc ≈ 0.14555 µs H: Hashing Cost = 0.0005, Ec: Encryption Cost = 0.0087, Dc: Decryption Cost	1440 bits.	-	-	0.045
P. K. Panda and S. Chattopadhyay [54], 2020	Embedded device: $4T_H + 4T_{EPM}$ Cloud server: $5T_H + 4T_{EPM}$ Total: $9T_H + 8T_{EPM}$ T_H: Hash Function Time. T_{EPM}: The Point Multiplication Time	1760 bits / 3 MSG	320 bits	-	-
Alzahrani et al. [57], 2020	$8T_{em} + 2T_{ea} + 6T_h \approx 13.42$ ms T_{em} = 2.226 ms: Cost of Point multiplication over ECC T_{ea} = 0.0288 ms: Cost of Point addition over ECC T_h = 0.0023 ms: Cost of hash function	168 Byte	-	-	-
Sowjanya et al. [58], 2020	Client: $3T_m + 1T_h + 1T_s \approx 92.035$ ms Application Provider: $6T_m + 3T_h + 1T_s \approx 38.291$ ms Total: 130.321 ms T_m: Cost of point multiplication over ECC T_h: Cost of hash function T_s : Symmetric encryption/decryption	Client: 2272 bits Application Provider: 1184 bits Total: 3456 bits	Client: 1248 bits Application Provider: 160 bits Total: 1408 bits	-	-

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

Kasyoka et al. [62], 2020	User: $T_{SM} + T_H$ 1 × 7.9 = 7.9 mJ Sensor: T_H Base station: $T_{SM} + T_H$ 1 × 7.9 = 7.9 mJ	864 bits	-	W_t= 5.64 mJ. W_r= 2.09 mJ.	-
Das et al. [63], 2019	7 T_{ecm} + 3 T_{eca} + 6 T_h = 94.414 ms. T_{ecm}: Cost of point multiplication over ECC ≈ 13.405 ms T_h: Cost of hash function ≈ 0.056 ms T_{eca}: Cost of point addition over ECC ≈ 0.081	3296 bits / 3 MSG	-	-	-

In [62] FPGA-based acceleration engine has been implemented for lightweight authentication based on elliptic curve cryptography. It consists of two interchangeable elliptic curves The proposed architecture presented a detailed experimental evaluation with low area based onVirtex-5 FPGA which used less than 1400 slices. It's suitable for constrained application devices such as IoT devices.

6. Conclusions

This paper presents literature reviews related to lightweight authentication based on elliptic curve cryptography from year to now. Through the study, it was clear that many of studies depend on simulation programs not implementation, and most of proposals have not implemented in true IoT network. Also, all security analysis must be performed on the proposed authentication mechanism with all possible attack models. In [69] an elliptic curve based authentication mechanisms were cryptanalyzed and failed in Confronting offline dictionary guessing attack, desynchronization attack, and privileged insider attack. Also, [70] succeeded to crack authentication scheme based on ECC where it also failed to confronting privilege insider attack, message insertion attack, and forward secrecy. it's important to test the scheme on the Distributed Denial of Service attacks in addition to existence of mutual authentication to prevent unavailability status of sensing devices. Finally, Most of IoT network devices are Heterogeneous and resource constrained which require considerations on compatibility and lightweight design.

References

1. M. El-hajj, A. Fadlallah, M. Chamoun and A. Serhrouchni "A Survey of Internet of Things (IoT) Authentication Schemes", Sensors, Vol.19, No.5, 2019, Art. No.1141, doi: 10.3390/s19051141.
2. M. G. Samaila, M. Neto, D. A. Fernandes, M. M. Freire and P. R. Inácio, "Challenges of securing Internet of Things devices: A survey", Security and Privacy Vol.1, No.2, 2018, doi: 10.1002/spy2.20.
3. S. Symanovich, "The future of IoT: 10 predictions about the Internet of Things," Accessed: Aug. 25, 2020. [Online]. Available: https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html.
4. M. Naeem, S. A. Chaudhry, K. Mahmood, M. Karuppiah and S. Kumari, "A scalable and secure RFID mutual authentication protocol using ECC for Internet of Things", International Journal of Communication systems, Vol.33, No.13, 2019, doi: 10.1002/dac.3906.
5. S. Rostampourab, M. Safkhanic, Y. Bendavida and N. Bagheri, "ECCbAP: A secure ECC-based authentication protocol for IoT edge devices", Pervasive and Mobile Computing, Vol. 67, Sep. 2020, doi: 10.1016/j.pmcj.2020.101194.

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

6. I. Abdellatif and Y. Bendavid, "Using a multi-perspective approach in the selection of an Internet-of-Things system," in: Proceedings of the 2018 International Conference of the Association of Global Management Studies, Montreal, vol. 1, pp. 46-52, 2018.
7. O. Abualghanam, M. Qatawneh and W. Almobaideen, "A Survey of Key Distribution in the Context of Internet of Things," Journal of Theoretical and Applied Information Technology, vol. 97, no. 22, pp. 3217–3241, 2019.
8. M. Saadeh, A. Sleit, K E. Sabri and W. Almobaideen, "Object Authentication in the Context of the Internet of Things: A Survey", Journal of Cyber Security and Mobility, Vol. 9, No.3, pp. 385–448, 2020.
9. S. Kavianpour, B. Shanmugam, S.Azam , M. Zamani , G. N. Samy and F. De Boer, "A Systematic Literature Review of Authentication in Internet of Things for Heterogeneous Devices", Journal of Computer Networks and Communications, Vol. 2019, Art. No. 5747136, doi :10.1155/2019/5747136.
10. W. M. Kang, S.Y. Moon and J. H. Park, "An enhanced security framework for home appliances in smart home", Human-centric Computing and Information Sciences, Vol.7, 2017, Art. No.6, doi :10.1186/s13673-017-0087-4.
11. S. Batool, N. Hassan, N. A. Saqib, and M. A. K. Khattak, "Authentication of Remote IoT Users Based on Deeper Gait Analysis of Sensor Data", IEEE Access, vol. 8, pp. 101784-101796, 2020, doi :10.1109/ACCESS.2020.2998412.
12. Z. Vahdati, S. M. Yasin, A. Ghasempour, M. Salehi, "Comparison of ECC and RSA Algorithms in IoT Devices", Journal of Theoretical and Applied Information Technology, Vol.97. No 16, Aug. 2019.
13. M. Ali, R. Reaz and M. G. Gouda, "Nonrepudiation protocols without a trusted party", 4th International Conference on Networked Systems, NETYS 2016, vol 9944, pp 1-15 May 2016, Springer 2016, doi : 10.1007/978-3-319-46140-3_1.
14. S. S. Dhanda, B. Singh, P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT", Wireless Personal Communications, Vol.112, pp. 1947–1980, 2020, https://doi.org/10.1007/s11277-020-07134-3
15. K. A. McKay, L. Bassham, M. S. Turan, and N. Mouha, ``Report on lightweight cryptography," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NISTIR 8114, Mar. 2017, doi : 10.6028/NIST.IR.8114.
16. Mohammed F. Albrawy, Ali Takieldeen, and Rashed Moktar El Awade. "Digital Data Encryption using Modified Method for Point Operations in ECC using Matlab" International Journal of Computer Science Engineering and Information Technology (IJCSEIT), ISSN (P): 2249-6831; ISSNI: 2249-7943, Vol. 4, Issue 3, PP: 159-170, Jun 2014, India.
17. C. Jiang, B. Li, and H. Xu, "An efficient scheme for user authentication in wireless sensor networks," in Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), pp. 438–442, Niagara Falls, Canada, May 2007, doi :10.1007/978-3-642-25255-6_34.
18. X. H. Le, M. Khalid, R. Sankar, and S. Lee, "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare," Journal of Networks, vol. 6, no. 3, pp. 355–364, 2011, doi: 10.4304/jnw.6.3.355-364.
19. S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmedy, F.Gagnon, and M. Guizaniz, "ECC-based Secure and Lightweight Authentication Protocol for Mobile Environment", IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 2019, pp. 1-6, doi :10.1109/INFOCOMWKSHPS47286.2019.9093756.
20. J. Joglekar, S. Bhutani, N. Patel, and P. Soman, "Lightweight Elliptical Curve Cryptography (ECC) for Data Integrity and User Authentication in Smart Transportation IoT System", International Conference on Sustainable Communication Networks and Application (ICSCN): Sustainable Communication Networks and Application, Lecture Notes on Data Engineering and Communications Technologies, vol 39. 2019, Springer, Cham. Doi :10.1007/978-3-030-34515-0_28
21. Sameh N. Gobran , Ali Takieldeen, and El-Sayed A. El-Badawy. "Digital Image Encryption Based on RSA Algorithm" International Organization of Scientific Research Journal of Electronics and Communication Engineering (IOSR-JECE), Volume 9, Issue 1, PP 69-73 , e-ISSN: 2278-2834, p- ISSN: 2278-8735, Jan. 2014, India
22. A. A. Alamr, F. Kausar, J. Kim and C. Seo, "A secure ECC-based RFID mutual authentication protocol for internet of things", The Journal of Supercomputing, Vol.74, pp. 4281–4294, 2018, springer, doi: 10.1007/s11227-016-1861-1.
23. P. K. Dhillon, S. Kalra, "Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things", Multimedia Tools and Applications, Vol.78, pp.22199–22222,2019, doi: 10.1007/s11042-019-7466-y.
24. Z. Liu, X. Huang, Z. Hu, M. K. Khan, H. Seo and L. Zhou, "On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age," in IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 3, pp. 237-248, 1 May-June 2017, doi: 10.1109/TDSC.2016.2577022.

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

25. Ali Takieldeen, Said H. Abd Elkhalik, Ahmed S. Samra,Mohamed A. Mohamed and Fahmi Khalifa."A Robust Security Scheme Based on Novel Encoding with LSB Steganography" The 2021 International Telecommunications Conference, ITC-Egypt'2021, July 13 - 15, 2021, ADC, Alexandria, Egypt
26. Unit 42, "2020 Unit 42 IoT Threat Report," Accessed: Aug. 26, 2020. [Online]. Available: https://unit42.paloaltonetworks.com/iot-threat-report-2020.
27. M. Nikooghadam and H. Amintoosi, "A secure and robust elliptic curve cryptography-based mutual authentication scheme for session initiation protocol", security and privacyVol.3, No.1,2019, doi: 10.1002/spy2.92.
28. E. Shaikh, I. Mohiuddin and A. Manzoor, "Internet of Things (IoT): Security and Privacy Threats," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp.1-6, doi: 10.1109/CAIS.2019.8769539.
29. M. Zaminkar and R. Fotohi, "SoS-RPL: Securing Internet of Things Against Sinkhole Attack Using RPL Protocol-Based Node Rating and Ranking Mechanism", Wireless Personal Communications, Vol.144, pp.1287–1312, 2020, doi: 10.1007/s11277-020-07421-z.
30. A. Biryukov, A. Shamir and D. Wagner, "Real time cryptanalysis of A5/1 on a PC, Fast Software Encryption (FSE)", LNCS, Vol. 1978, pp. 1–18, 2001, New York: Springer.
31. L. JIAO1, Y. HAO and D. FENG, "Stream cipher designs: a review", SCIENCE CHINA Information Sciences, Vol.63, No.3, 2020, doi: 10.1007/s11432-018-9929-x.
32. C. Manifavas, G. Hatzivasili, K. Fysarakis and Y. Papaefstathiou, "A survey of lightweight stream ciphers for embedded systems", Security and Communication Networks, Vol. 9, pp. 1226– 1246, 2016, doi: 10.1002/sec.1399.
33. N. AlFardan, D. J. Bernstein, K.G. Paterson, B. Poettering and J. C. Schuldt. "On the security of RC4 in TLS", 22nd USENIX Security Symposium, USENIX Security, Washington DC, USA, pp. 305–320, 2013.
34. J. Massey, "Shift-register synthesis and BCH decoding", IEEE Transactions on Information Theory, Vol.15, No.1, pp.122–127, 1969, doi: 10.1109/TIT.1969.1054260.
35. S. B. Sadkhan and Z. Hamza, "Proposed Enhancement of A5/1 stream cipher," 2019 2nd International Conference on Engineering Technology and its Applications (IICETA), Al-Najef, Iraq, 2019, pp. 111-116, doi: 10.1109/IICETA47481.2019.9013008.
36. R. Bonnerji, S. Sarkar, K. Rarhi and A. Bhattacharya, "COZMO - A new lightweight stream cipher", PeerJ Preprints, Vol.6, doi: 10.7287/peerj.preprints.6571v1.
37. B. J. Mohd and T. Hayajneh, "Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques," in IEEE Access, vol. 6, pp. 35966-35978, 2018, doi: 10.1109/ACCESS.2018.2848586.
38. D. Sehrawat, N. S. Gill and M. Devi, "Comparative Analysis of Lightweight Block Ciphers in IoT-Enabled Smart Environment," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2019, pp. 915-920, doi: 10.1109/SPIN.2019.8711697.
39. A. Biswas, A. Majumdar, S. Nath, A. Dutta and K. L. Baishnab, "LRBC: a lightweight block cipher design for resource constrained IoT devices", Journal of Ambient Intelligence and Humanized Computing, 2020, doi: 10.1007/s12652-020-01694-9.
40. Y. Su, Y. Gao, O. Kavehei and D. C. Ranasinghe, "Hash Functions and Benchmarks for Resource Constrained Passive Devices: A Preliminary Study," 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kyoto, Japan, 2019, pp. 1020-1025, doi: 10.1109/PERCOMW.2019.8730835.
41. B. Seok, J. Park and J. H. Park, "A Lightweight Hash-Based Blockchain Architecture for Industrial IoT", Applied Sciences, vol.9, No.18, 2019, doi: 10.3390/app9183740.
42. A. Kumar, A. Aggarwal, N. J. Ahuja and R. Singhal "Design and Analysis of Elliptic Curve Cryptography-Based Multi-Round Authentication Protocols for Resource-Constrained Devices", Intelligent Communication, Control and Devices. Advances in Intelligent Systems and Computing, vol.989, pp.707-717, 2019, Springer, Singapore, doi: 10.1007/978-981-13-8618-3_72.
43. S. Adhikari and S. Ray, "A Lightweight and Secure IoT Communication Framework in Content-Centric Network Using Elliptic Curve Cryptography", Recent Trends in Communication, Computing, and Electronics, Lecture Notes in Electrical Engineering, vol.524, pp. 207-216, Dec.2018, Springer, Singapore, doi: 10.1007/978-981-13-2685-1_21.
44. Y. Jiang, Y. Shen and Q. Zhu, "A Lightweight Key Agreement Protocol Based on Chinese Remainder Theorem and ECDH for Smart Homes", vol. 20, no.5, 2020, Sensors, doi: 10.3390/s20051357.

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

45. D. Noori, H. Shakeri and M. N. Torshiz, "Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment", EURASIP Journal on Information Security, No.13, 2020 doi: 10.1186/s13635-020-00114-x
46. A. Shafiq, I. Altaf, K. Mahmood, S. Kumari and C. M. Chen, "An ECC Based Remote User Authentication Protocol", Journal of Internet Technology, vol.21, pp.285-294, 2020, doi:10.3966/160792642020012101024.
47. Y. S. Wei and J. h. Chen. "Tripartite Authentication Protocol RFID/NFC Based on ECC", International Journal of Network Security, Vol.22, No.4, PP.664-671, July 2020, doi: 10.6633/IJNS.202007 22(4).15.
48. X. Qin, Y. Huang and X. Li, "An ECC-based access control scheme with lightweight decryption and conditional authentication for data sharing in vehicular networks", Soft Computing, 2020, doi: 10.1007/s00500-020-05117-x.
49. J. Guruprakash and S. Koppu, "EC-ElGamal and Genetic Algorithm-Based Enhancement for Lightweight Scalable Blockchain in IoT Domain," in IEEE Access, vol. 8, pp. 141269-141281, 2020, doi: 10.1109/ACCESS.2020.3013282.
50. L. C. Thungon, N. Ahmed, S. C. Sahana and M. I. Hussain, "A lightweight authentication and key exchange mechanism for IPv6 over low-power wireless personal area networks-based Internet of things", Transactions on Emerging Telecommunications Technologies, 2020, doi: 10.1002/ett.4033.
51. A. Aziz and K. Singh, "Lightweight Security Scheme for Internet of Things", Wireless Personal Communications, vol.104, pp.577-593, 2019, doi: 10.1007/s11277-018-6035-4.
52. A. Kumar and A. K. Jain, "A Lightweight Authentication Scheme for RFID Using ECC", 4th International Conference on Internet of Things and Connected Technologies (ICIoTCT), Advances in Intelligent Systems and Computing, vol 1122, pp. 177-183, 2019, Springer, Cham., doi: 10.1007/978-3-030-39875-0_19.
53. M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, vol. 8, pp. 52018-52027, 2020, doi: 10.1109/ACCESS.2020.2980739.
54. P. K. Panda and S. Chattopadhyay, "A secure mutual authentication protocol for IoT environment", Journal of Reliable Intelligent Environments, vol.6, pp.79-94, 2020, doi: 10.1007/s40860-020-00098-y.
55. P. G. Chilveri and M. S. Nagmode, "A novel node authentication protocol connected with ECC for heterogeneous network", Wireless Networks, vol.26, pp.4999–5012, 2020, doi: 10.1007/s11276-020-02358-4.
56. S. Chatterjee and S. G. Samaddar, "A Robust Lightweight ECC-Based Three-Way Authentication Scheme for IoT in Cloud", Smart Computing Paradigms: New Progresses and Challenges, vol. 767, pp.101-111, 2019, doi: 10.1007/978-981-13-9680-9_7
57. B. A. Alzahrani, S.A. Chaudhry, A. Barnawi, A. Al-Barakati, and T. Shon, "An Anonymous Device to Device Authentication Protocol Using ECC and Self Certified Public Keys Usable in Internet of Things Based Autonomous Devices", Electronics vol.9, no.3, 2020, doi: 10.3390/electronics9030520.
58. K. Sowjanya, M. Dasgupta and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems", International Journal of Information Security, vol.19, pp.129–146, 2020, doi: 10.1007/s10207-019-00464-9.
59. Z. Xie and L. Jiang, "An improved authentication scheme for Internet of things", IOP Conf. Series: Materials Science and Engineering, vol. 715, 2020, doi: 10.1088/1757-899X/715/1/012031.
60. E. Gyamfi, J. A. Ansere and L. Xu, "ECC Based Lightweight Cybersecurity Solution for IoT Networks Utilising Multi-Access Mobile Edge Computing," *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC),* Rome, Italy, 2019, pp. 149-154, doi: 10.1109/FMEC.2019.8795315.
61. C.A. L. Nino, A. D. Perez and M. M. Sandoval, "Lightweight elliptic curve cryptography accelerator for internet of things applications", Ad Hoc Networks, vol.103, no.1, 2020, doi: 10.1016/j.adhoc.2020.102159.
62. P. Kasyoka, M. Kimwele and S. M. Angolo, "Multi-user broadcast authentication scheme for wireless sensor network based on elliptic curve cryptography", Engineering Reports, vol.2, no.7, 2020; doi: 10.1002/eng2.12176.
63. A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues and Y. Park, "Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment," in *IEEE Access*, vol. 7, pp. 55382-55397, 2019, doi: 10.1109/ACCESS.2019.2912998.
64. B. Seok, J.C. S. Sicato, T. Erzhena, C. Xuan, Y. Pan and J. H. Park, "Secure D2D Communication for 5G IoT Network Based on Lightweight Cryptography", Applied Sciences , vol.10, no.1, 2020, doi: 10.3390/app10010217.
65. L. ZHOU, C. SU, Z. HU, S. LEE and H. SEO, "Lightweight Implementations of NIST P-256 and SM2 ECC on 8-bit Resource-Constraint Embedded Device" ACM Transactions on Embedded Computing Systems, Vol. 18, No. 3, Article 23, 2019, doi: 10.1145/3236010.

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021

66. G. Gaubatz, JP. Kaps and B. Sunar, "Public Key Cryptography in Sensor Networks—Revisited", Ad-hoc and Sensor Networks. ESAS 2004. Lecture Notes in Computer Science, vol.3313, 2004, Springer, Berlin, Heidelberg, doi:10.1007/978-3-540-30496-8_2
67. Ali Takieldeen, Said H. Abd Elkhalik, Ahmed S. Samra, Mohamed A. Mohamed and Fahmi Khalifa. "A Robust and Hybrid Cryptosystem for Identity Authentication" MDPI Information, Vol 12, Issue 3, ISSN 2078-2489, July2021, Switzerland.
68. A. Gawade and R. Vinchhi, "Lightweight Random Number Generation for Elliptic Curve Cryptography for Use in IoT", pp. 67-73, 2020, Advanced Computing Technologies and Applications, Algorithms for Intelligent Systems, Springer, Singapore, doi: 10.1007/978-981-15-3242-9_7.
69. J. Mo, Z. Hu, and Y. Lin, "Cryptanalysis and Security Improvement of Two Authentication Schemes for Healthcare Systems Using Wireless Medical Sensor Networks", Security and Communication Networks, Volume 2020, Art. ID. 5047379, doi: doi.org/10.1155/2020/5047379.
70. C. Patel and N. Doshi, "Cryptanalysis of ECC-based key agreement scheme for generic IoT network model," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-7, doi: 10.1109/ICCCNT45670.2019.8944674.

DOI: 10.5281/zenodo.5301587
Received: March 02, 2021 Accepted: July 22, 2021