sciendo

BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **19**, No 1
Sofia • 2019 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2019-0008

Security of Low Computing Power Devices: A Survey of Requirements, Challenges & Possible Solutions

Anuj Kumar Singh[1], *B. D. K. Patro*[2]

[1]*Dr. A. P. J. Abdul Kalam Technical University, Lucknow, U. P., India*
[2]*Rajkiya Engineering College, Kannauj, U. P., India*
E-mails: anujbtechcs@gmail.com bdkpatro@rediffmail.com

***Abstract*:** *Security has been a primary concern in almost all areas of computing and for the devices that are low on computing power it becomes more important. In this paper, a new class of computing device termed as Low Computing Power Device* (*LCPD*) *has been defined conceptually. The paper brings out common attributes, security requirements and security challenges of all kinds of low computing power devices in one place so that common security solutions for these can be designed and implemented rather than doing this for each individual device type. A survey of existing recent security solutions for different LCPDs hasve been presented here. This paper has also provided possible security solutions for LCPDs which include identification of countermeasures against different threats and attacks on these devices, and choosing appropriate cryptographic mechanism for implementing the countermeasures efficiently.*

***Keywords*:** *Computing power, security, requirements, challenges, solutions.*

1. Introduction

With the new era of technology in communication, the numbers of users have increased rapidly utilizing different kinds of computing devices depending upon the nature of communication. The computing devices used today are heterogeneous in nature, having different technical specifications and computing ability. Furthermore, the computing occurs in an open environment and becomes ubiquitous. Providing security in these types of surroundings has become a fundamental need. Ensuring security of communication involving heterogeneous devices depends upon the computational power of these devices, as there is a trade-off between the performance and the security features to implement. It is inevitably important to analyze the computing power of the devices used in communication so that appropriate security solutions can be designed and implemented.

1.1. Notion of computing power

Generally speaking, computing power of a device is the measure that how fast a machine can perform some computation. The computing power of a machine with

respect to the time taken depends upon the three attributes – processing speed, memory required, and the bandwidth used. Since the inception of computer age computing devices have been given specific names including micro computer, mini computers, mainframe computers and supercomputers, but with the technological advancements new computing devices like mobiles, tablets, pagers, embedded computers, game consoles and, sensors emerged which have now become the backbone of the communication infrastructure. Moreover, the evolvement of IoT [1], which is an integrated environment of different embedded devices, machines and appliances with Internet connectivity, has given birth to a new era of computing. So due to many types of computing and communication devices existing today, from security point of view, there is a need of defining a new class of computing devices Low Computing Power Device (LCPD) which has been defined and explained in the next subsection.

1.2. Specification of LCPD

Definition. A LCPD can be defined as a device that has very low processing capability, limited memory, less bandwidth and restricted power.

Typically, three types of devices can be considered to belong to LCPD category; these are Wireless Sensor Nodes [2], RFID (Radio Frequency IDentification) Tags & Receivers [3] and Smart Cards [4] since all these have limited processing capacity, memory, bandwidth and power. Different types of computers and communication devices have been invented for a variety of applications and these devices differ in processing capability, memory or storage, bandwidth, power and applications supported. A comparison of category of computing devices has been made and it is shown in Table 1.

Table 1. Comparison of classes of computing devices

No	Class of Computing Device	Processing Speed	Memory	Applications
1	Supercomputer	10 s peta FLOPS	100 s of Tebibyte	Weather forecasting, Complex Scientific Calculations, Massively Parallel Processing, etc.
2	Mainframe Computer	10000 s of MIPS	10 s of GB	Bulk data processing, ERP, Market Statistics, etc.
3	Minicomputer	1000 s of MIPS	10 s of GB	Control, Instrumentation, Human Interaction, Communication Switching, etc.
4	Microcomputer (Desktop, Laptops, Tablets, Smartphones, PDAs, Palmtops)	100 s of MIPS	Few GB	Personal Computations
5	Low Computing Power Device (LCPD) (Wireless Sensors, RFID, Smart Cards)	Up to few MIPS	Few 100 s of MB	Security Systems, Information Gathering, Access Control, Tracking, Asset Management and many more

In Table 1 typical average processing speed and memory for a category has been considered: 1 Tebibyte is 2^{40} bytes; MIPS – Million Instructions Per Second; GB – GigaByte; MB – MegaByte.

It can be analyzed from Table 1 that low computing power devices have a very low processing speed of few MIPS and limited memory up to few 100 s of MB, which is a major concern while designing security schemes for these devices. The detailed specification of LCPD is shown in Table 2 that shows that typically a device belonging to LCPD class possess a processing speed of few 10 s MHz, flash memory up to 1 MB and random access memory of few 100 s of kB. This specification is on an average and in some cases, these parameters may be less or more depending upon the area of application for which the device has been manufactured. It is important to note that from security viewpoint cryptographic support including both symmetric key cryptography and asymmetric key cryptography can be provided for the applications, which are using LCPDs. In Table 2 the last column states that lightweight cryptographic methods involving AES, ECC, SHA 1, etc., can be designed and implemented in a computing environment utilizing low computing power devices. In Table 2: AES is Advanced Encryption Standard; ECC – Elliptic Curve Cryptography; SHA1 – Secure Hash Algorithm 1.

Table 2. Specification of LCPD

No	Type of LCPD	CPU Clock (MHz)	Flash Memory (MB)	RAM (KB)	Cryptographic Support
1	Wireless Sensor Nodes [2]	Few 10 s	Up to 1	Few 100 s	AES, ECC, SHA1
2	RFID Tags [3]	1-5	Up to 1	Few 100 s	AES, ECC, SHA1
3	Smart Cards [18]	1-5	Up to 1	Few 100 s	AES, ECC, SHA1
Class LCPD		Up to few 10 s	Up to 1	Few 100 s	AES, ECC, SHA1

1.3. Constraints for LCPD

A massive number of LCPDs are being used in day-to-day communications for different applications but unfortunately, from security point of view these devices suffer from the following three constraints.

1.3.1. Less computing capacity

LCPD possess very limited processing ability with only few MIPS and restricted memory up to only few 100 MB and due to this reason, implementing security schemes that provide all the necessary security attributes have been very exigent for the applications involving LCPDs.

1.3.2. Limited power

Certain versions of LCPDs operate on a power source typically a battery. Since the battery is a limited power resource, extreme care has to be taken while implementing all the necessary applications including security algorithms, i.e., efficient and lightweight implementation is required.

1.3.3. Unreliable communication

Since LCPDs are integrated with the applications that often work in open wireless environment, they are exposed to different kinds of threats and attacks. This raises the requirement of implementing strong security mechanisms to thwart all the attacks.

1.4. Advantages and disadvantages of different LCPDs

A brief overview, application areas, advantages and disadvantages of each kind of LCPD is presented in this subsection. Table 3 shows the comparison of advantages and disadvantages of different types of LCPDs.

Table 3. Comparison of advantages and disadvantages of different LCPDs

Type of LCPD	Advantages	Disadvantages
Wireless sensors [2]	• Enable monitoring in harsh and hostile areas • No fixed infrastructure required • Flexibility in implementation • Sensor based networks are scalable • Less implementation cost	• Less computational capacity • Low power • Security vulnerabilities • Slow operation speed • Complexity in configuration • Signal attenuation at large distances
RFID tags [3]	• Track moving objects • Provide location information • Faster in operation • Easy implementation	• Less computational capacity • Low power • Security vulnerabilities • Electromagnetic interference • Short range • Higher cost than comparative technologies
Smart cards [4]	• Multiple usage of a single card • Larger memory • Longer life • Higher security than RFID and Sensors • Less cost of operations	• Less computational capacity • Low power • Security vulnerabilities • Risk of viruses • Theft issues • More production cost

1.4.1. Wireless sensors

Sensor nodes, the fundamental building blocks of wireless sensor networks are capable of sensing, computing and communicating the information to the base station or gateway [6]. Generally, the sensor nodes are equipped with a microcontroller, sensor, radio transceiver, memory, battery, antenna and supporting circuit. The main function of a sensor node is to sense the environment where it is deployed for monitoring, gather the required data and communicate the data to the neighbouring nodes or gateway. There are many areas where wireless sensors networks are used for controlling and monitoring including process management, environmental sensing, health monitoring, industrial monitoring, disaster prevention, military applications, infrastructure security and many more. The main advantage of wireless sensors is that they can be easily placed for monitoring in harsh and hostile areas such as mountains, forests, and seas. Moreover, wireless sensor networks do not use fixed infrastructure, are scalable, possess less implementation cost and are flexible. The disadvantages of the wireless sensor include security vulnerabilities, less

computational capability, low power, slow computation, complexity in configuration and signal attenuation at large distances.

1.4.2. Radio Frequency IDentification (RFID) tags

RFID is an automatic identification and data capture technology based on radio frequency electromagnetic signals. Out of other automatic identification technologies like bar codes, magnetic stripes, and chip cards, RFID is considered most significant due to its ability to detect moving objects. The two important components of RFID technology are RFID tags and RFID receiver. An RFID tag consisting an antenna and an integrated circuit receives the radio frequency signal and process the data. A RFID receiver consisting a radio frequency module and a microprocessor interrogates the tags to authenticate them and collect the information. The application of RFID includes healthcare, manufacturing, logistics, inventory, animal tagging, postal tracking, access control and many more. The main advantage of RFID technology is that it can track moving objects without requiring line of sight. Furthermore, RFID tags can store information, provide the location information, faster in operation and can be easily implemented. The disadvantages of RFID are security vulnerabilities, electromagnetic interference, short range, less computational capability, low power, and more cost.

1.4.3. Smart cards

The Smart card consists of an integrated circuit and are used to provide identification information, perform authentication, storing data and application processing. Smart cards can be used in implementing secure identification, healthcare systems, secure payments, and mobile applications. The advantages of smart cards are high security, larger memory storage, reliability, less cost of operations, longer life, and using a single card for multiple applications. Disadvantages include the risk of viruses, theft issues, a greater cost of production, security and privacy issues.

2. Security requirements of LCPDs

With the use of different types of devices along with LCPDs in the ubiquitous computing environment, security has become an essential need of the hour, as this kind of computing is vulnerable to serious attacks. The four basic security features which must be provided in all types of communication are confidentiality, integrity authentication, and non-repudiation [5], but the properties of low computing devices enforce the inclusion and implementation of many more security attributes. In [6-10] different authors have discussed the security requirements of wireless sensor networks. L o p e z, R o m a n and A l c a r a z [11] have presented a comprehensive survey on the security of Wireless Sensor Networks (WSN) and discussed the security threats and security requirements of WSN. They identified that the security attributes that a WSN implements must include confidentiality, integrity, authentication, authorization, availability, data freshness, forward security, self-organization, and non-repudiation. Similarly, the security requirements for RFID systems have also been analyzed in [12-16].

Knospe and Pohl [17] have brought out that confidentiality, integrity, availability, authentication, and anonymity are necessary security features for the systems using RFID tags and readers. In addition to these security features, forward secrecy is a security attribute that must be considered for RFID systems as they operate in the wireless medium. Smart cards [18] have also similar security requirements as that of WSN and RFID. By studying [19-22], one can conclude that for smart card based systems confidentiality, integrity, authentication, and non-repudiation along with forward secrecy are the security features, which must be implemented successfully. A comparison of the security requirements of different LCPDs is shown in Table 3.

The major security requirements common to all kinds of low computing power devices highlighted in Table 3 are briefly explained below.

2.1. Confidentiality

The data or message sent in a communication must be kept secret i.e. the same must be converted into an incomprehensible form by the LCPD so that it is understood the intended recipient only. Data confidentiality can be achieved by encrypting the data with a secret key and then sharing secret key securely with the receiver.

2.2. Integrity

Since LCPDs may generate confidential information, it must be ensured that the information being communicated is not altered or modified by an opponent while in transit. For achieving the integrity of the information appropriate hash function may be used.

2.3. Authentication

Authentication is required to ensure that the message has been sent by the right sender and not by an intruder or opponent. If there are many parties involved in the communication then it becomes more challenging to authenticate each other, as in the case of WSNs. Authentication can be implemented by either using MAC or by using public key schemes like digital signature.

2.4. Availability

The availability of LCPD and the network in which the device is working should be maintained. It must be ensured that LCPDs are not overloaded with unnecessary computations and they should be protected from the adversary who can force these devices to enter into large number of unnecessary computations.

2.5. Forward secrecy

This is the property which ensures that even when the long term secret session key is compromised the adversary cannot deduce the past session keys, i.e., the recorded encrypted past communications cannot be decrypted. A random one-time session secret key should be used to facilitate forward secrecy in the process of encryption.

2.6. Non repudiation

This is the assurance that after sending/receiving the message sender/receiver cannot deny that the message has not been sent/received. The non-repudiation can be achieved by using digital certificates provided by a trusted third party.

Table 4. Security requirements of different LCPDs

No	Device	CON	INT	AUT	AVA	FWS	NRP	AUTH	FRE	SOR
1	Wireless sensors [11]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2	RFID tags [17]	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
3	Smart cards [22]	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Common security attributes – CON, INT, AUT, AVA, FRS, NRP										

It can be analyzed that security requirements for RFID and smart cards are the same. However, in the case of WSNs, there are three additional security requirements – authorization, data freshness, and self-organization. Therefore generalized security schemes for LCPDs can be designed which satisfy common security requirements as mentioned in Table 4 and then some remaining specific security features can be implemented additionally (CON is Confidentiality; INT – Integrity; AUT – Authentication; AVA – Availability; FWS – Forward Security; NRP – Non Repudiation; AUTH – Authorization; FRE – Freshness; SOR – Self Organization).

3. Challenges in the security of LCPDs

As discussed earlier LCPDs suffer from the constraints of low computing capacity, limited power, and unreliable communication. These constraints enforce the two major security challenges – threats and attacks faced by the systems using LCPDs and the choice of cryptographic mechanism to implement necessary security features.

3.1. Threats and attacks

In [23-27] the authors have presented the studies and surveys on different kinds of attacks on wireless sensor networks. However, Dhakne and Chatur [28] have given the detailed analysis and divided the attacks on WSNs in five categories based on different perspectives – layers, authentication, privacy, and others. Security& privacy issues and challenges for RFID have been discussed in [29-32], which provides knowledge about the potential attacks and threats for RFID systems. Khattab et al. [33] mentioned that the attacks on RFID could be broadly classified into three categories namely physical threats, channel threats and system threats. Hoon Ko and Caytiles [19] have given a review on smart card security in which they have divided the attacks on smart cards into four categories – logical attacks, physical attacks, side channel attacks, and other attacks. Pippal, Jaidhar and Tapaswi [34] have mentioned that the password guessing attack, impersonation attack, session attack, replay attack, DoS attack, and attack on forward secrecy can be attempted on the authentication schemes of smart cards. Mahanta, Azad and Khan [35] have mentioned that power analysis attacks are also a threat for smart cards. Some new security aspects of high-density smart cards have been discussed by

H a n d s c h u h and T r i c h i n a [36] and they have explained the interaction of flash memory with other memories since many applications reside on high-density smartcards. The various categories and the specific threats and attacks on different low computing environments are shown in Table 5 and by analyzing these threats and attacks it is to state that many attacks are common to all kinds of LCPDs.

Table 5. Attacks on different LCPDs

<table>
<tr><th colspan="2">Attacks on WSN [28]</th><th colspan="2">Attacks on RFID [33]</th><th colspan="2">Attacks on Smart cards [19]</th></tr>
<tr><td>Category of Attack</td><td>Specific Attack</td><td>Category of Attack</td><td>Specific Attack</td><td>Category of Attack</td><td>Specific Attack</td></tr>
<tr><td rowspan="3">Attacks based on different perspectives</td><td>Outsider vs Insider</td><td rowspan="4">Physical Threats</td><td>Tag Disabling</td><td rowspan="4">Logical Attacks</td><td>Hidden Commands</td></tr>
<tr><td>Passive vs Active</td><td>Tag Modification</td><td>Parameter Poisoning</td></tr>
<tr><td>Node Capture Attack</td><td>Tag Cloning</td><td>File Access</td></tr>
<tr><td rowspan="5">Attacks on Layers</td><td>Physical Layer Attacks (Jamming, Tampering, Path based DoS)</td><td>Reverse Engineering & Physical Exploration</td><td>Malicious Applets</td></tr>
<tr><td>Link Layer Attacks (Collision)</td><td rowspan="6">Channel Threats</td><td>Eavesdropping</td><td rowspan="4">Physical Attacks</td><td>Chemical Solvents and Staining Materials</td></tr>
<tr><td>Network Layer Attacks (Black Hole, Sybil, Spoofing, Sinkhole, Wormhole, Hello Flood)</td><td>Snooping</td><td>Reverse Engineering</td></tr>
<tr><td>Transport Layer Attacks (Flooding, Desynchronization)</td><td>Skimming</td><td>Probe Stations</td></tr>
<tr><td>Application Layer Attacks</td><td>Replay Attack</td><td>Focused Ion beam</td></tr>
<tr><td>Attacks on Secrecy & Authentication</td><td>Node Replication</td><td>Relay Attack</td><td rowspan="5">Side Channel Attacks</td><td>Differential Power Analysis</td></tr>
<tr><td rowspan="2">Attacks on Privacy</td><td>Eavesdropping</td><td>Jamming</td><td>Power Glitching</td></tr>
<tr><td>Traffic Analysis</td><td rowspan="4">System Threats</td><td>Spoofing</td><td>Password Cracking</td></tr>
<tr><td rowspan="2">Other Attacks</td><td>Bad/Good Mouthing</td><td>Tracing/ Tracking</td><td>Denial of Service</td></tr>
<tr><td>On-Off</td><td>Password Cracking</td><td>Eavesdropping</td></tr>
<tr><td></td><td></td><td>Denial of Service</td><td rowspan="3">Other Attacks</td><td>Interruption of Operations</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Covert Transactions</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Dual Modes</td></tr>
</table>

Therefore it will be logical to group all the common attacks on LCPDs into two broad categories namely Physical Attacks and Information Security Attacks as mentioned in Table 16. Physical attacks are the attacks in which the device is

physically modified, disabled or cloned. Information security attacks involve the attacks which are used to steal or modify confidential information.

3.2. Choice of cryptographic mechanism

Due to the lack of resources in LCPDs it is a continuous challenge to select the appropriate cryptographic mechanism which provides all the necessary security features mentioned in Table 4. Moreover, at the same time, the chosen mechanism must be able to counter the information security threats and attacks pointed out in Table 16. The cryptographic mechanisms, which are potential candidates to be used in securing LCPDs, have been discussed in this sub-section.

3.2.1. Symmetric Key Cryptography (SKC)

In SKC [37] the same key is used for encrypting and decrypting the message. The symmetric key algorithms like DES and AES can be used to provide confidentiality of the message being transmitted. The two fundamental reasons that make secret key encryption attractive for LCPDs are – first computational complexity and communication overhead are less second, the cryptographic support for implementing algorithms like AES is available in LCPDs as shown in Table 2.

According to the survey performed by Singh and Shende [113] and Mushtaq et al. [114], a comparison of different symmetric key encryption algorithms has been made and shown in Table 6. Mitali, Kumar and Sharma [115] have performed the analysis of computational time taken by different symmetric key encryption algorithms on numerous input sizes, which have been demonstrated in Fig. 1. With the use of symmetric key encryption protection from eavesdropping and snooping can be provided. The first limitation of symmetric key cryptography is the requirement of the huge number of keys when a large number of entities are involved in the communication. The second limitation is the secure distribution of the secret key among all parties, for which another secure mechanism is required.

Table 6. Comparison of different symmetric key encryption algorithms

Symmetric Key Algorithm	Structure	Key Size (bits)	No of Rounds	Block Size (bits)	Security	Speed
DES	Feistel	56	16	64	Already Broken	Slow
3 DES	Feistel	112, 168	48	64	Adequate	Very Slow
AES	Substitution/ Transposition	128, 192, 256	10, 12, 14	128	Excellent	Fast
Blowfish	Feistel	32-448	16	64	Excellent	Fast

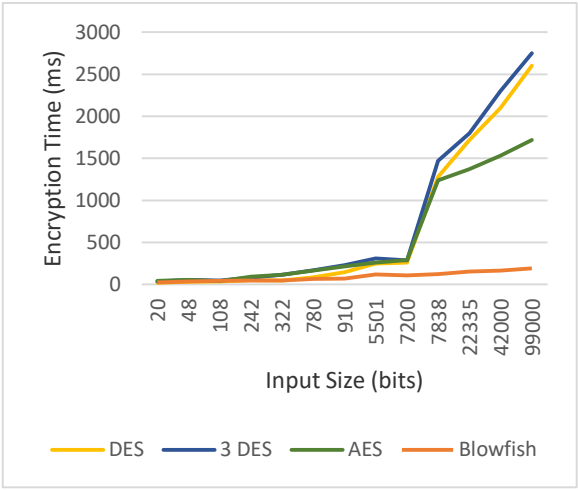


Fig. 1. Analysis of encryption time of different symmetric key encryption algorithms

3.2.2. RSA Based Cryptography (RBC)

This is a public key cryptographic mechanism in which first, a key pair is generated then one key is used for encryption and the other is used for decryption. The advantage of RSA based schemes [38] is that confidentiality and authentication can be provided using the same scheme. This mechanism can be implemented to protect against eavesdropping, spoofing, skimming and replay attacks. Although the number of keys required is less as compared to symmetric key cryptography, but RSA based schemes involve modular exponentiation, which consumes more machine cycles and add extended bits in the encrypted plaintext. Due to this reason, it is not wise to use RSA based schemes for LCPDs.

3.2.3. Elliptic Curve Cryptography (ECC)

ECC [39, 40] is a public key cryptographic approach, which has been found a suitable candidate to be used for LCPDs due to the requirement of smaller key size for the same echelon of security as compared to the RSA based mechanisms. The comparison of required key size for different cryptographic mechanisms is shown in Table 9. Furthermore, the strength of ECC is based on ECDLP (Elliptic Curve Discrete Logarithm Problem) which is intractable. ECC can be used to provide all major security features including confidentiality, non-repudiation, authentication, and forward secrecy along with providing a shield from eavesdropping, snooping, spoofing, skimming, power analysis and replay attack. S. R. S i n g h, A. K. K h a n and T. S. S i n g h [116] have performed the key generation, encryption, decryption, signing, and verification operations on 25 bytes input for RSA and ECC both, using Intel i3 processor of 3.10 GHz and 4 GB RAM. The analysis of the computational time of these operations on different key sizes is shown in Tables 7 and 8 for RSA and ECC respectively. With this analysis, one can easily deduce that the time for all the computations and size of resulted ciphertext in ECC is much lesser than that of RSA. Hence, ECC is suitable for implementing security functionalities in LCPDs.

Table 7. Computational time of operations in RSA for different key sizes

Key Size (bits)	Time in Key Generation (ms)	Time in Encryption (ms)	Time in Decryption (ms)	Time in Signing (ms)	Time in Verification (ms)	Ciphertext Size (bits)
112	2,825,151.941	2,840.752	260,099.529	74,699.908	1,703.145	616
128	10,270,890.31	4,405.311	593,957.338	185,208.775	3,382.025	925
192	10,267,678.287	17,218.556	8,837,759.875	229,3216.586	18,538.609	2,311

Table 8. Computational time of operations in ECC for different key sizes

Key Size (bits)	Time in Key Generation (ms)	Time in Encryption (ms)	Time in Decryption (ms)	Time in Signing (ms)	Time in Verification (ms)	Ciphertext Size (bits)
112	36,239.910	1,450.239	10,231.465	39,564.742	44,990.073	248
128	32,403.603	1,848.262	11,607.045	4,662.882	54,761.921	248
192	32,457.264	2,061.037	12,794.513	86,548.193	110,636.252	256

3.2.4. Pairing Based Cryptography (PBC)

With the introduction of Identity Based Encryption by B o n e h and F r a n k l i n [41] based on Weil Pairing, the bilinear pairing has attracted most of the cryptographic researchers since pairing offers many security features. Specifically pairing based cryptography provides key management, requires less key size in bits and most importantly it is more secure than other cryptographic mechanisms [42]. Pairing based on elliptic curves can endow with confidentiality, authentication, non–repudiation and forward secrecy concurrently defending against eavesdropping, snooping, spoofing, skimming, power analysis and replay attack. However, C a o and L i u [81] have highlighted that in pairing-based cryptography there is a need of generating large size parameters, which require a lot of computing power and due to this reason pairing-based schemes are not suitable for LCPDs.

3.2.5. Lightweight hash functions

Hash function [43] is an important primitive used in cryptography that takes a string of arbitrary size as input and produces a fixed length hash code also called a message digest.

The integrity of the message can be assured using the hash function like SHA 1. Although SHA 1 works well with all types of cryptographic mechanisms discussed in point No 3.2.1-3.2.4 but for LCPDs there is a requirement of using lightweight hash functions. SPONGENT [44], GLUON FAMILIY [45], PHOTON FAMILIY [46], HASH-ONE [47] and Neeva [48] are some of the lightweight hash functions, which can be used with any cryptographic mechanism. The advantage of using these is the production of less number of extended bits in the computation and hence they are suitable for LCPDs.

A comparison of different cryptographic mechanisms against some evaluation parameters is publicized in Table 9. Through this analysis, one can observe that each cryptographic mechanism has some strengths and weaknesses i.e. the mechanism like SKC is fast but it does not provides all the security functions while others like ECC and PBC provide many security features but are slow in computation. From LCPDs point of view choosing any one of the four SKC, RBC, ECC or PBC will not work. Appropriate cryptographic mechanism along with lightweight building blocks

inheriting the advantages of symmetric key cryptography and asymmetric key cryptography have to be used for LCPDs such that it provides all the necessary security functions and protects against the security attacks listed in Table 16, at the same time taking less computational time and less communication overhead (Co is Confidentiality; Au – Authentication; Nr – Non-repudiation; Ke – Key Exchange; n – number of parties in communication).

Table 9. Comparison of cryptographic mechanisms

No	Evaluation parameters	Cryptographic mechanism		
		SKC	RBC	ECC/PBC
1	Approach	Symmetric	Asymmetric	Asymmetric
2	Computational Cost	Low	High	High
3	Communication Overhead	Low	High	Low
4	Order of No of Keys	$O(n^2)$	$O(n)$	$O(n)$
5	Key Distribution	A big problem	Complex	Simple
6	Key bits (same security level)	80	1024	160
7	Speed of Key Generation	Speedy	Slow	Speedy
8	Basic Security Functions	Co	Co, Au, Nr, Ke	Co, Au, Nr, Ke
9	Complexity	$O(n)$	$O(n^3)$	$O(n^2)$
10	Memory Requirement	Small	Very Large	Less than RBC but more than SKC

4. Recent low cost security solutions for LCPDs

Wireless sensors, RFID tags, and smart cards are the LCPDs, which have been used widely in many critical applications, and therefore designing efficient security solutions for these environments have always been a primary concern for the researchers and industries. In this section, a survey of recent low cost security solutions for wireless sensors, RFID tags, and smart cards is performed. The analysis presented in this survey is based on the literature provided and proofs given by authors.

4.1. Recent security protocols for wireless sensors

Key exchange and authentication protocols for Wireless Sensor Networks (WSN) are the two major focus areas which have been given due attention in recent research works. In this sub-section a comparison of latest low cost key exchange and authentication protocols for wireless sensor networks is accomplished with respect to computational time, the bandwidth required, security features and resistance against different attacks. For all protocols 160 bit ECC has been used and the three communicating parties are the user, gateway and server. Table 10 demonstrates the computational time and bandwidth required for each WSN protocol. W u et al. [90] have mentioned that on a 64-bit i7 processor of 2.5 GHz with 8 GB RAM, the time taken in an elliptic curve point multiplication is 0.427576 ms, time in single hash computation is 0.005174 ms and time consumed in a single encryption/decryption is 0.0214835 ms.

Table 10. Comparison of costs of recent ECC based WSN protocols

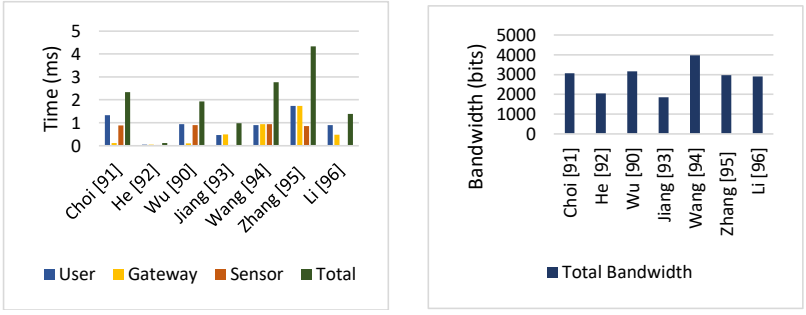
Protocol	No of operations performed												Total time (ms)	Band-width (bits)
	User			Gateway			Sensor			Total				
	p	*h*	*e*	*p*	*h*	*e*	*p*	*h*	*e*	*p*	*h*	*e*		
Choi et al. [91]	3	9	0	0	1	5	2	6	0	5	16	5	2.328082	3072
He, Kumar and Chilamkurti [92]	0	8	0	0	9	0	0	6	0	0	23	0	0.119002	2048
Wu et al. [90]	2	11	1	0	11	2	2	4	1	4	26	4	1.930762	3168
Jiang et al. [93]	1	8	0	1	12	0	0	5	0	2	25	0	0.984502	1856
Wang, Xu and Sun [94]	2	8	0	2	11	1	2	11	1	6	30	2	2.763643	3968
Zhang, Xu and Wei [95]	4	4	0	4	5	0	2	1	0	10	10	0	4.327500	2976
Li et al. [96]	2	8	0	1	9	0	0	4	0	3	21	0	1.391382	2912

In Table 10 *p* is the number of elliptic curve point multiplications; *h* – number of hash computations; *e* – number of encryption/decryption operations.

Table 11. Comparison of security features of recent ECC based WSN protocols

Protocol	Security attributes							Resistance against attacks					
	MUT	CON	SKE	KEP	ANO	FSP	UNT	RPL	IMP	SVA	SNI	ODA	INA
Choi et al. [91]	✓	✓	✓	✓	×	✓	×	✓	✓	×	✓	×	×
He, Kumar and Chilamkurti [92]	×	×	✓	✓	✓	✓	×	✓	×	×	✓	×	×
Wu et al. [90]	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓
Jiang et al. [93]	✓	✓	✓	×	×	✓	✓	✓	✓	✓	✓	✓	✓
Wang, Xu and Sun [94]	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓
Zhang, Xu and Wei [95]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Li et al. [96]	✓	✓	✓	×	×	✓	✓	✓	✓	✓	✓	✓	✓

In Table 11 MUT is the Mutual authentication; CON – Confidentiality; SKE – Secure Key Establishment; KEP – Key Privacy; ANO – Anonymity; FSP – Formal Security Proof; UNT – Untraceability; RPL – Replay attack; IMP – Impersonation attack; SVA – Stolen Verifier Attack; SNI – Sensor Node Impersonation; ODA – Offline Dictionary Attack; INA – Insider attack; ✓ – Provided; × – Not Provided.



(a) (b)

Fig. 2. Computational time of WSN protocols (a); bandwidth of WSN protocols (b)

Computational time for each protocol has been calculated by counting the number of elliptic curve point multiplications, number of hash computations and number of encryption or decryptions carried out by the user, gateway and sensor in each protocol.

Then these counts are multiplied by the time taken in a single operation and then added finally to calculate total computational time. Bandwidth has been calculated by adding the size of messages sent by the user, gateway and sensor for every protocol. Fig. 2 shows the graphical analysis of computational time and bandwidth required for different WSN protocols respectively. Table 11 compares different WSN protocols with respect to the security attributes provided and resistance against attacks made on to the system.

4.2. Recent security protocols for RFID

Recent security protocols for RFID based on Elliptic Curve Cryptography (ECC) have been compared as these provide secure authentication, which is a primary requirement of the communication between RFID tags and reader. For all protocols it is assumed that the connection between the tag and reader is wireless while there is a wired connection between the reader and the server. Furthermore, 160 bit ECC is used in each protocol and the tag memory is 504 bytes.

Table 12. Comparison of costs of recent ECC based RFID protocols

Protocol	Computational cost				Communication cost (bits)		Storage cost (bits)	
	No of scalar multiplications		Computational time (ms)					
	Tag	Reader	Tag	Reader	Tag	Reader	Tag	Reader
Zhang et al. [98]	4	2	256	128	960	160	1600	1440+480*n*
Zhao [99]	5	5	320	320	640	640	1760	1120+480*n*
Liao and Hsiao [100]	5	5	320	320	640	640	1920	1280+800*n*
Almar, Kausar and Kim [101]	4	5	256	320	640	960	1920	1120+320*n*
Jin et al. [102]	4	3	256	192	640	640	1600	1120+320*n*
Zheng et al. [103]	3	4	192	256	640	640	2080	1760+320*n*
Dinarvand and Barati [104]	3	3	192	192	800	640	1760	1120+800*n*

Table 12 shows the comparison of computational time, communication cost and storage cost of different RFID protocols. Computational time of ECC based protocols is based on the number of elliptic curve scalar multiplication operation executed since it is the most time consuming operation and the time taken by other operations is negligibly small in comparison to elliptic curve scalar multiplication.

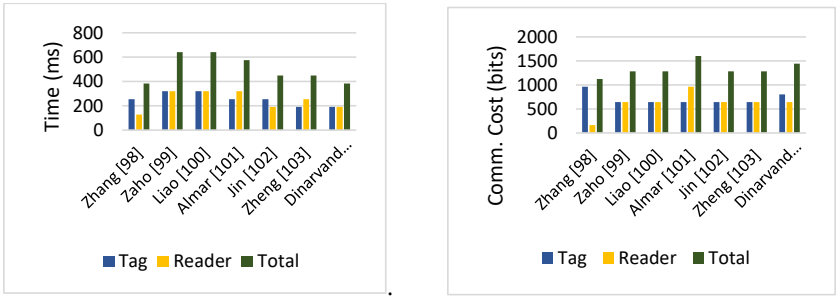
Computational time of each protocol has been calculated based on the fact that for a 5 MHz tag it takes 64 ms to compute a single elliptic curve scalar multiplication operation [97].

In Table 13 MUT is the Mutual authentication; CON – Confidentiality; ANO – Anonymity; SCA – Scalability; FWS – Forward security; LOC – Location privacy; INT – Data integrity; MIT – Man in the middle attack; RPL – Replay attack; IMP – Impersonation attack; KEC – Key compromise attack; LCT – Location tracking attack; DOS – Denial of service attack; CLO – Cloning attack; SSP – Server spoofing attack; DES – Desynchronization attack; ✓ – Provided; × – Not Provided.

Table 13. Comparison of security features of recent ECC based RFID protocols

Protocol	Security attributes								Resistance against attacks								
	MUT	CON	ANO	AVL	SCA	FWS	LOC	INT	MIT	RPL	IMP	KEC	LCT	DOS	CLO	SSP	DES
Zhang et al. [98]	×	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	×	×
Zhao [99]	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓
Liao and Hsiao [100]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓	✓	✓	✓	✓
Almar, Kausar and Kim [101]	✓	✓	✓	×	×	✓	✓	×	✓	✓	✓	✓	✓	×	✓	✓	×
Jin et al. [102]	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓
Zheng et al. [103]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dinarvand and Barati [104]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

The communication cost has been computed based on the size of messages exchanged by the tag and the reader. Storage cost is another important parameter to evaluate the security protocols for RFID because if the storage cost of a tag or the reader is high then the protocol will not be scalable. Assuming that there are n number of tags in the system, storage cost for the tag and the reader is computed by calculating the size of the parameters they have to store. Fig. 3a and b show the graphical analysis of computational time and communication cost of different RFID protocols respectively. In Table 13, secure RFID protocols have been compared with respect to the security features they provide and the attacks that they can counter.



(a) (b)

Fig. 3. Computational time of RFID protocols (a); communication cost of RFID protocols (b)

4.3. Recent Security protocols for Smart cards

Secure authentication protocols for smart cards are of great importance as many server applications use smart cards to authenticate the users. In this sub-section recent research works over authentication protocols for smart cards have been compared with respect to their computational time and communication cost. The methodology of calculating the computational time is the same as discussed in Subsection 4.1. The smart card protocols [106-109] are based on modular exponentiations whereas protocol [105] and [110-112] are based on elliptic curves. According to Xie et al. [105] on Intel i5 processor of 2.5 GHz with 8 GB RAM it takes 3.043 ms for

executing one modular exponentiation and 2.501 ms for a single elliptic curve point multiplication operation.

The cost of other operations has been ignored in this analysis as the time taken by them is reasonably small in comparison to modular exponentiation and elliptic curve point multiplication. Computational cost of the smart card protocols has been publicized in Table 14 (p is the number of elliptic curve point multiplications; x – number of modular exponentiations), and the security of these protocols has been compared in Table 15 (MUT is the Mutual authentication; SKA – Session Key Agreement; FWS – Forward security; TFA – Two factor authentication; FSP – Formal Security Proof; RPL – Replay attack; KKA – Known Key Attack; IMP – Impersonation attack; SIA – Server Impersonation Attack; INA – Insider attack; PGA – Password Guessing Attack; ✓ – Provided; × – Not Provided). Fig. 3 presents the graphical analysis of computational of different smart card security protocols.

Table 14. Computational costs of recent Smart card protocols

Protocol	No of operations performed						Time (ms)		
	User		Server		Total		User	Server	Total
	p	*x*	*p*	*x*	*p*	*x*			
Pippal, Jaidhar and Tapaswi [106]	0	3	0	4	0	7	9.129	12.172	21.301
Yeh [107]	0	2	0	4	0	6	6.086	12.172	18.258
Wang et al. [108]	0	2	0	1	0	3	6.086	3.043	9.129
Odelu, Das and Goswami [109]	0	3	0	3	0	6	9.129	9.129	18.258
Chaudhry et al. [110]	3	0	3	0	6	0	7.503	7.503	15.006
Xie et al. [105]	3	0	3	0	6	0	7.503	7.503	15.006
Truong et al. [111]	2	0	2	0	4	0	5.002	5.002	10.004
Zhao, Li and Jiang [112]	2	0	2	0	4	0	5.002	5.002	10.004

Table 15. Comparison of security features of recent Smart card protocols

Protocol	Security attributes					Resistance against attacks						
Pippal, Jaidhar and Tapaswi [106]	✓	✓	✓	×	×	✓	✓	✓	×	×	✓	×
Yeh [107]	×	×	✓	×	×	✓	✓	✓	×	✓	✓	×
Wang et al. [108]	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	×
Odelu, Das and Goswami [109]	✓	✓	✓	✓	✓	✓	✓	×	×	×	✓	✓
Chaudhry et al. [110]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Xie et al. [105]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Truong et al. [111]	✓	✓	✓	✓	×	✓	✓	✓	×	×	✓	×
Zhao, Li and Jiang [112]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

From the survey carried out in 4.1, 4.2 and 4.3 it can be observed that security mechanisms for LCPDs do exist but they do not provide resistance against all the attacks mentioned in Table 16. Furthermore, there is a trade-off between computational time and security functionalities, i.e., the protocols that consume less time are unable to provide the desired security functions and those providing adequate security take more time. Computational time efficient security schemes can be designed by using techniques like signcryption [80] which provide resistance against all the attacks shown in Table 16 and provide all necessary security attributes.

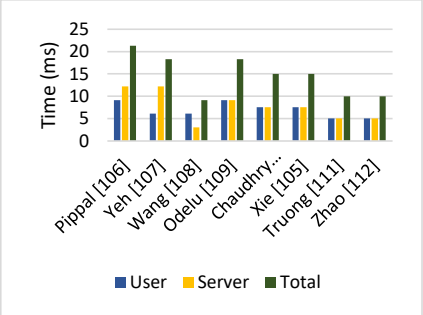


Fig. 4. Computational time of Smart card protocols

Table 16. Common attacks on LCPDs and their countermeasures

Category of Attack	Specific Attack	Elucidation	Countermeasures
Physical Attacks	Disabling	Disabling the device temporarily or permanently	MAC using shared secret key
	Tampering	Adversary can remove or modify the device	Building a secure zone and using sealed tamper resistant case
	Cloning	Deploying the duplicate device for intrusion	Cryptographic fingerprinting, MAC using shared secret key
	Jamming	Adversary can use a radio signal to interfere with the device signal and thus causing the electromagnetic jamming	Spread spectrum technologies, Polarization of antenna
	Reverse Engineering	By reverse engineering, technical details of the device can be obtained which enables cloning	Cryptographic fingerprinting, Strong cryptographic algorithm
Information Security Attacks	Eavesdropping	Listening to the channel to obtain confidential information	Lightweight encryption algorithm
	Snooping	Reading the information from a device without owner's knowledge	Lightweight encryption and authentication algorithm
	Spoofing	A malicious device may use the ID of some legal device to mimic the legitimate behavior to some other device	Lightweight authentication mechanism
	Skimming	Attacker observes the interactions between the legitimate sender and the receiver and then make a fake document, which appears real to the device	Symmetric authentication using shared key, Hash-lock
	Replay Attack	A malicious device replays the secret information to do fraud	Hash code with parameter occurrence (using lightweight hash function)
	Denial of Service	The attacker targets a specific device to block it by forcing the same to do massive computations	Lightweight authentication mechanism & Physical Unclonable Function
	Side Channel Attacks	Attacker analyzes the physical characteristics of the device to extract secret information	Publicized in Table 17

5. Possible security solutions for LCPDs

Security solutions for low computing power devices must address the two challenges elaborated in Subsections 3.1 and 3.2 of this paper. First, they should be able to defeat the threats and attacks by using suitable countermeasures and second, they should use efficient cryptographic mechanism to implement the same.

5.1. Countermeasures against attacks

The very first step towards providing security solutions for LCPDs is to realize the countermeasures to the physical attacks and information security attacks as mentioned in Table 16. For each specific attack, appropriate mechanism must be identified and efficiently implemented to thwart that attack. A brief description and possible solutions for each type of attack are explained in the next sub-sections.

5.1.1. Disabling

In disabling attack, the attacker causes the device to enter a state so that it cannot be identified by the back end-server or any other device in the network [50]. A disabling attack can be prevented with the use of a shared secret key only between the device and the second party involved in the communication. The second party generates the challenge value and the response is generated by the device using the shared secret key. The device using an efficient Message Authentication Code (MAC) like Poly1305 can produce this response [51].

5.1.2. Tampering

This is a physical security attack in which an attacker can try to modify the device or even remove it from the system. A device can be protected from it by limiting the access to the device by building a secure zone around it [52]. Barenghi et al. [53] have mentioned that the physical access to a device can be restricted by keeping the device in a sealed tamper-resistant case so that when an unauthorized entity tries to tamper the device it cannot do so and the act of tampering is detected.

5.1.3. Cloning

In cloning attack, the adversary creates the replica of the device to produce an unauthorized effect. Burmester and Medeiros [50] has mentioned that it is an integrity attack in which the opponent somehow captures the identifying information of the device and then uses this information with the replica device to penetrate the network or system. Bu et al. [54] have presented a detailed survey on the prevention and detection of clones in RFID in which they highlighted the main idea, strengths, and weaknesses of each type of solution. Khan, Mohamad Saad and Aalsalem [55] have analyzed the clone detection methods in WSN and pointed out the drawbacks of existing schemes. They concluded that none of the schemes works well in a mobile WSN. Santis and Soriente [56] proposed a fingerprinting mechanism to protect the cards from cloning. For all types of LCPDs there are two ways to counter cloning attack first is the use of a secret key to generate MAC so that device can be identified by the server and network. The second possible

solution is to use a cryptographic fingerprint, which can be generated using a hash code on the set of data related to the device. In this case, if the device is cloned then the hash code for the device will be different and the cloning can be detected easily.

5.1.4. Jamming

In this type of attack an attacker, obstruct the usual behavior of the device using electromagnetic or radio frequency signals which are generated from a jamming device. In [57, 58] the authors have given a comprehensive survey on the vulnerabilities and countermeasures against jamming attacks in WSN. L o p e z et al. [59] and K h a t t a b et al. [3] have mentioned that jamming attack can be categorized as passive jamming and active jamming. Passive jamming is generally unintentional and occurs when the interference is produced by the unwanted noise in the communication environment such as noise from power supplies. Active Jamming is a deliberate act of creating electromagnetic signal by an adversary to disrupt the actual communication to and from the device. Jamming attack can be prevented by using spread spectrum technologies like FHSS or DSSS and polarization of antenna.

5.1.5. Reverse engineering

This attack is made to exploit the internal structure and detailed functioning of the device so that the communication with the device can be intercepted or the device can be cloned. B o k s l a g [60] pointed out that to protect the device against reverse engineering strong cryptographic algorithms and authentication mechanism must be implemented. However, it will increase the power and computational requirements of the device. Cryptographic fingerprints are also a solution to reverse engineering as discussed in point No 5.1.3.

5.1.6. Eavesdropping

It is one of the most common attacks on the privacy of information being transferred. This attack is passive in nature and involves listening to the channel secretly to retrieve sensitive information. Eavesdropping becomes more serious and effective attack when combined with traffic analysis [28]. Since LCPDs operate in the unreliable wireless environment and may be involved in communicating important secret information, it becomes important to protect them from eavesdropping. D a i et al. [61] classified eavesdropping attack as active eavesdropping and passive eavesdropping. In passive eavesdropping, the malicious device just listens to the channel to grab the confidential information, whereas in active eavesdropping the attacker masquerade themselves as friendly nodes and then captures the information by sending queries to the target device. Prevention from eavesdropping attack can be assured by providing confidentiality to the transmitted information. For LCPDs it will be sensible to use the lightweight encryption algorithm rather than traditional measures. B h a r d w a j, K u m a r and B a n s a l [62] have surveyed and compared different lightweight cryptographic algorithms for data security. They mentioned that ECC based encryption algorithms are best suited for LCPDs as the size of the key required is very less in comparison to RSA based schemes. Furthermore, ECC based

algorithms provide more security in comparison to the encryption algorithms based on Feistel Network.

5.1.7. Snooping

This attack involves the illegitimate reading the identity of the device and its data without the knowledge of the owner [33]. Snooping is different from eavesdropping in the sense that snooping take place when the data stored on the device is stolen by the attacker while in eavesdropping the attacker reads the transmitted information between two legitimate devices. Snooping can be countered by providing two security features – confidentiality and authentication i.e. the data on the device must be stored in encrypted form and if any party wants to access the data that must be authenticated. Lightweight encryption and authentication algorithms as mentioned in point No 5.1.6 must be implemented for LCPDs to prevent them from snooping.

5.1.8. Spoofing

In spoofing attack, the attacker changes the MAC address of the target device with its own MAC address. This attack is very serious as the adversary can target important nodes in the system like access point in a network and from there it can damage many nodes connected to the access point. Similarly, spoofing can be used to attack RFID systems by changing the identity of a tag with the identity of the attacker. Alotaibi and Elleithy [63] have revealed that one obvious solution to prevent from spoofing is to provide authentication but it involves large computations, causes overhead and consumes more power. Khemissa, Tandjaoui and Bouzefrane [64] proposed an ultra-lightweight authentication mechanism for the heterogeneous environment, which consumes less energy at the same time providing resistance against different attacks. Lightweight authentication is a better solution towards protection from spoofing attacks.

5.1.9. Skimming

This attack arises when the documents related to the identity of the device are authenticated. The attacker monitors the interaction between the device and the authenticating party, and then a fake document is created by the attacker which can be used in masquerading or cloning the device [33]. Haver [65] has highlighted the two approaches to thwart skimming attack. The first approach called as symmetric authentication that makes use of a shared secret key to generate MAC for a challenge generated by the communicating party, which is then used for authentication before sending or receiving any data. The second approach is to use Hash-lock [66], which is based on the hash function. In this approach initially, all the devices are in locked mode and reply only by using metaID, which is a hash code of the actual ID. The authorized device has a list of metaID and ID pairs so that they can verify the identity of the device.

5.1.10. Replay attack

This attack involves recording the messages and information being transferred between the two legitimate parties and then replaying the same later on to produce an

unauthorized effect. In LCPDs replay attacks are very serious as they can degrade the performance of the network or target a particular device to bring it down. Few solutions that have been implemented to counter replay attack include time-stamping, OTP, nonce and dynamic updating the information [33]. In a recent work S h a r m a and H u s s a i n [67] have investigated that these solutions are either complex or not secure enough to defy replay attack. They proposed a mechanism, which provides protection from the replay attack. This mechanism computes a hash code for each message and stores it into a table. Upon receiving a message, the hash value for the message is computed and searched in the table. If the computed hash value is new then the corresponding entry is made in the table, but if the entry for the hash value is found then certainly, it is the replayed message and is rejected. This approach will be more effective for LCPDs if lightweight hash functions mentioned in point No 3.2.5 are used in computing the hash value.

5.1.11. Denial of Service (DoS)

DoS attack is very common in the present computing environment in which a malicious device targets a legitimate device and makes it perform a huge number of unnecessary computations. Moreover, when another genuine device wants to communicate the attacked device it becomes unavailable as it remains busy with spurious computations. This attack is more severe for LCPDs due to their constraints of computing power. According to W a n g et al. [68] many security solutions have been given to prevent DoS attacks but from LCPDs point of view, the use of PUF (Physical Unclonable Function) is most significant. The idea of PUF was given by G a s s e n d et al. [69]. PUF consumes less power, provides unclonability and are unpredictable. These features make PUF a promising mechanism to counter against DoS attacks in an authenticated environment or network of LCPDs.

5.1.12. Side channel attacks

Side channel attacks have great significance in LCPDs since these generally occur in a wireless environment and due to these attacks, there is a large probability of information leaking out. According to S t a n d a e r t [70] side channel attacks are the category of attacks in which an attacker attempts to obtain confidential information by analyzing physically leaked timing information, power consumption or electromagnetic radiation. K h a n and M a h a n t a [71] have classified side channel attacks in four categories namely timing attack, electromagnetic attack, fault analysis attack, and power analysis attack. In Timing attack the adversary tries to get the information about the time taken by the device in different computations and then makes statistical analysis from this timing information to guess about the key. G e et al. [72] have presented a recent survey on timing attacks in which potential techniques to counter these attacks have been explained which include constant time techniques, injecting noise, enforcing determinism, partitioning time, partitioning hardware resources and auditing. Generally, all LCPDs operates on power and hence the electric current in them creates an electromagnetic field and the information carried by this electromagnetic field can be analyzed by an attacker to steal confidential data. R o h t a g i [73] have mentioned countermeasures to electromagnetic attack including circuit redesign to reduce EM emissions, EM shielding, creating physically

secure zones and reducing signal information. In the operation of LCPDs faults in their operations are either due to some invalid input or due to an invalid computation made, in both the cases the faulty output is produced. In fault analysis attacks these faulty outputs are analyzed to obtain secret information. K h a n and M a h a n t a [71] have mentioned that the only countermeasure to fault analysis attack is to restart the process again instead of continuing with the faulty output. P o p p, O s w a l d and M a n g a r d [74] have provided the introduction of power analysis attacks and their countermeasures. According to them power analysis attacks attempts to get the secret information based on power consumption by the device, as the power consumption by different cryptographic operations is different. Power analysis attacks are further divided into two sub-categories namely Simple Power Analysis (SPA) and Differential Power Analysis (DPA). In SPA the adversary analyzes power consumption of cryptographic operations carried out by a device in order to obtain secret information possibly the key used. SPA uses single power trace or multiple power traces by giving the inputs and observing the power consumed on those inputs. The potential countermeasures for SPA are hiding and masking [74]. In hiding the power consumption of almost every operation is kept same so that the attacker cannot identify the operation. Masking involves randomizing the intermediate values processed by the device in a way that these are independent of actual values. M a h a n t a, A z a d and K h a n [75] have defined DPA based on the fundamental that the power consumed by computing logic has some statistical relationship with the internal bit operations. Large numbers of power traces are used by DPA. In contrast to SPA any prior information about the device under DPA attack is not needed. They identified hiding, blinding, masking, noise insertion, temporal desynchronization and algorithmic measures as resisting techniques against DPA. The summary of all types of side channel attacks along with their possible countermeasures are shown in Table 17 (SPA is the Simple Power Analysis, DPA – Differential Power Analysis).

Table 17. Types of side channel attacks and their countermeasures

No	Type of side channel attack		Elucidation	Countermeasures
1	Timing attack		Analyzes the time taken by the device in different computations.	Constant time techniques, injecting noise, determinism, partitioning time & hardware, auditing
2	Electromagnetic attack		Analyzes electromagnetic field of the device to obtain secret information.	Circuit redesign, EM shielding, creating secure zone
3	Fault analysis attack		Analyzes faulty outputs to get confidential information.	Restart the process again on getting faulty output
4	Power analysis attack	SPA	Analyzes the power traces on the inputs given.	Hiding, masking
		DPA	Involves statistical analysis of large number of power traces	Hiding, blinding, masking, noise insertion, temporal de-synchronization and algorithmic measures

5.2. Cryptographic mechanisms for LCPDs

There are two possibilities to design and implement appropriate cryptographic schemes for LCPDs. First, to implement necessary security features by using Hybrid Cryptography and second is to use an integrated mechanism called signcryption which provides many security attributes simultaneously with very less cost as compared to other approaches.

5.2.1. Using hybrid security mechanism for LCPDs

Hybrid cryptographic mechanism [49] is the amalgamation of multiple cryptographic approaches inheriting advantages of each of these, i.e., instead of using any one cryptosystem for providing all the security features the idea is to create a mechanism which provides different security attributes using different mechanisms discussed in Subsectios 3.2.1 to 3.2.5. Like AES which is a symmetric key algorithm can be used to provide confidentiality and ECC which belongs to public key cryptography can be used for key exchange and authentication. Some authors have proposed hybrid cryptographic approaches to implement different security features. Dubai, Mahesh and Ghosh [76] developed a hybrid security algorithm based on Dual RSA, Elliptic Curve Digital Signature Algorithm and MD5 that provides integrity, confidentiality, and authentication. Chourasia and Singh [77] proposed a hybrid encryption algorithm for textual data by combining DES and RSA, which requires less key size. However, this approach only provides confidentiality. Prakash and Rajput [78] have given an efficient hybrid cryptographic approach for WSNs by utilizing the advantages of AES and Elliptic Curve Cryptography. It provides confidentiality and secure key sharing between the sender and the receiver. Rachmawati et al. [79] proposed a hybrid cryptosystem by combining Tiny Encryption algorithm and LUC algorithm. This approach provides integrity and confidentiality of the message.

Table 18. Summary of hybrid cryptographic schemes

Hybrid scheme	Algorithms used	Security features	Limitations
Dubai, Mahesh and Ghosh [76]	Dual RSA, ECDSA, MD5	CON, INT, AUT	Missing NRP, AVA, FWS, KE
Chourasia, Singh [77]	DES, RSA	CON, INT	Missing AUT, NRP, AVA, FWS, KE
Prakash, Rajput [78]	DES, ECC	CON, KE	Missing INT, AUT, NRP, AVA, FWS,
Rachmawati et al. [79]	Tiny encryption algorithm, LUC	CON, INT	Missing AUT, NRP, AVA, FWS, KE

The summary of discussed hybrid security schemes is shown in Table 18 (CON is Confidentiality; INT – Integrity; AUT – Authentication; NRP – Non Repudiation; AVA – Availability; FWS – Forward Security; KE – Secure Key Exchange), from which it is clear that these schemes fail to provide all the major security attributes required for LCPDs, i.e., if all security attributes are to be implemented then more than one scheme with different levels of security should be used. This will increase the cost to a large amount. We can conclude that if only a few security features are

required then hybrid security schemes will be suitable for LCPDs but for implementing them all simultaneously requires a mechanism that is more efficient.

5.2.2. Using signcryption for LCPDs

The concept of signcryption, which provides both confidentiality and authentication simultaneously in one single step, was established by Zheng [80]. Before signcryption the approach was to apply signature first and then encrypt the information. Zheng proved that signcryption saves 50% computational cost and 85% of communication overhead than the conventional signature-then-encryption approach. Over the years many signcryption schemes have been proposed which are based on RSA, elliptic curve cryptography or pairing-based cryptography. RSA based signcryption schemes involve modular exponentiation operation which is very time consuming, and so they are not suitable for LCPDs. Cao and Liu [81] have highlighted that in pairing based cryptography there is a need of generating large size parameters which requires a lot of computing power and due to this reason pairing based signcryption schemes are also not suitable for LCPDs. The only remaining possible efficient solution for LCPDs is to use signcryption schemes based on elliptic curve cryptography. The very first ECC based signcryption scheme was proposed by Zheng and Imai [82] in which they claimed a saving of 58% in computational time and 40% in communication overhead than signature-then-encryption. This scheme provides confidentiality, integrity, and unforgeability but fails to offer forward secrecy, public verification and non-repudiation directly. Hwang, Lai and Su [83] developed an efficient signcryption scheme based on elliptic curve cryptography that offers all the major security attributes including forward secrecy and public verification. Toorani and Shirazi [84] proposed an elliptic curve based signcryption mechanism that offers all the necessary security features but it takes more computational and communication cost than the existing ones. Hagras, Saied and Aly [88] presented a signcryption key management scheme for WSNs based on elliptic curve, which offers all the major security features but takes the huge computational cost. Bala, Sharma and Verma [85] designed an ECC based signcryption scheme, which solves the problem of key exchange in WSN. A signcryption scheme based on elliptic curve discrete logarithmic problem has been given by Amounas, Sadki and Kinani [89], which satisfies all major security attributes and takes less computational cost as compared to other schemes. However, this scheme has no constraint on the selection of curve parameters. Chaudhry et al. in [86] designed a signcryption scheme based on ECDLP, but this protocol does not provide forward secrecy and public verifiability. Based on security features and computational cost, a comparative analysis of the discussed elliptic curve based signcryption schemes are shown in Table 19. Xie et al. [105] have revealed that on Intel i5 processor of 2.5 GHz with 8 GB RAM it takes 2.501 ms for a single elliptic curve point multiplication operation. The time consumed in other operations is negligibly small in comparison to elliptic curve point multiplication and has been ignored in the analysis.

Table 19. Comparison of elliptic curve based signcryption schemes

Signcryption scheme	Security features							Computational cost											
								No of operations performed											Time, ms
								Signcryption						Unsigncryption					
	CON	INT	AUT	UNF	NRP	FWS	PUV	Pm	Pa	Mu	Dv	Ad	Hc	Pm	Pa	Mu	Dv	Ad	Hc
Zheng and Imai [82]	✓	✓	✓	✓	×	×	×	1	0	1	1	1	2	2	1	2	0	0	2	7.503
Hwang, Lai and Su [83]	✓	✓	✓	✓	✓	✓	✓	2	0	1	0	1	1	3	1	0	0	0	1	12.505
Toorani and Shirazi [84]	✓	✓	✓	✓	✓	✓	✓	2	0	1	0	2	1	4	1	0	0	0	2	15.006
Hagras, Saied and Aly [88]	✓	✓	✓	✓	✓	✓	✓	3	0	0	1	1	4	4	1	0	0	0	3	17.507
Bala, Sharma and Verma [85]	✓	✓	✓	✓	×	×	×	1	0	0	1	1	2	3	1	0	0	0	1	10.004
Amounas, Sadki and Kinani [89]	✓	✓	✓	✓	✓	✓	✓	2	1	1	0	0	1	1	1	0	0	0	1	7.503
Chaudhry et al. [86]	✓	✓	✓	✓	✓	✓	×	1	1	0	1	0	0	2	1	0	0	0	0	7.503

In Table 19 CON is Confidentiality; INT – Integrity; AUT – Authentication; NRP – Non Repudiation; FWS – Forward Security; UNF – Unforgeability; PUV – Public Verification; Pm – Point multiplication; Pa – Point addition; Mu – Scalar Multiplication; Dv – Division; Ad – Scalar Addition; Hc – Hash computation; ✓ – Provided; × – Not Provided.

By this analysis, it can be observed that each of the elliptic curve based signcryption scheme mentioned have some drawback as some schemes are not able to provide all major security attributes simultaneously while some of them acquire more cost and overhead. Another observation is that not all of these schemes use lightweight hash functions in their computation. They all use SHA1 for implementing hash functions. If lightweight building blocks in signcryption schemes based on elliptic curve cryptography are used, the computational cost and communication overhead will be further reduced making these schemes more suitable for LCPDs. Therefore, the problem of designing efficient lightweight signcryption schemes based on elliptic curve for LCPDs is now open for the research community. The approach to design efficient security solutions for LCPDs should be logically divided into two steps. In first step, generalized lightweight signcryption schemes based on ECC must be designed for LCPDs providing all the common security attributes mentioned in Table 3. Then in second step the security mechanism for remaining device specific security features should be implemented based on their requirements. This is equivalent to implementing security functionality at two layers. One layer is common to all types of LCPDs and the second layer is flexible for the specific type of LCPD shown in Table 2.

6. Conclusion and future scope

The computing age has changed rapidly and the applications are now integrating different computing devices at one place like Internet of Things. This integration has forced to develop common security solutions suitable for all kinds of computing devices. The main focus of this paper is on the security issues of different low computing power devices. This paper has surveyed the security issues of LCPDs systematically in five sections. The very first section has explained the term LCPD along with the technical specifications. A comparison of the advantages and disadvantages of different LCPDs has also been discussed in this section. The second section has identified the common security requirements of LCPDs, which include confidentiality, integrity, authentication, non-repudiation, availability and forward secrecy. The third section has elaborated the two major challenges for LCPDs, which are threats & attacks against LCPDs and choice of cryptographic mechanism. The fourth section has presented a comprehensive survey of recent security solutions for different LCPDs. The last section of the paper has provided possible security solutions for LCPDs. Recent research references have been used in the paper to present the work effectively before interested readers and researchers. The facts and figures presented in this paper are of great importance for the academicians and researchers working in the area of security. Finally, the paper has unwrapped the problem of designing lightweight signcryption schemes based on elliptic curve for LCPDs, in front of the research community.

References

1. Mukhopadhyay, S. C., N. K. Suryadevara. Internet of Things: Challenges and Opportunities. – In: S. C. Mukhopadhyay, Ed. Smart Sensors. Measurement and Instrumentation. Vol. **9**. Switzerland, Springer, 2014, pp. 1-17.
2. Kateeb, A. E., A. Ramesh, L. Azzawi. Wireless Sensor Nodes Processor Architecture and Design. – In: Proc. of International Conference on Advanced Information Networking and Applications (AINA'08) – Workshops, Okinawa, 2008, pp. 892-897.
3. Khattab, A., Z. Jeddi, E. Amini, M. Bayoumi. Introduction to RFID. – In: Md. Ismail, Md. Sawan, Eds. RFID Security. Analog Circuits and Signal Processing. Springer, AG, 2017, pp. 3-26.
4. Mohammed, L. A., A. R. Ramli, V. Prakash, M. B. Daud. Smart Card Technology: Past, Present, and Future. – International Journal of the Computer, the Internet and Management, Vol. **12**, 2004, No 1, pp. 12-22.
5. Marin, G. A. Network Security Basics. – IEEE Security & Privacy, Vol. **3**, 2005, No 6, pp. 68-72.
6. Selmic, R. R., V. V. Phoha, A. Serwadda. Wireless Sensor Networks. Chapter 4 – Security in WSNs. Springer, AG, 2016.
7. Juneja, D., A. Sharma, A. K. Sharma. Wireless Sensor Network Security Research and Challenges: A Backdrop. – In: A. Mantri, S. Nandi, G. Kumar, S. Kumar, Eds. High Performance Architecture and Grid Computing (HPAGC'2011). Communications in Computer and Information Science. Vol. **169**. Berlin, Springer, 2011, pp. 406-416.
8. Panda, M. Security in Wireless Sensor Networks Using Cryptographic Techniques. – American Journal of Engineering Research, Vol. **5**, 2014, No 1, pp. 50-56.
9. Walters, J. P., Z. Liang, W. Shi, V. Chaudhary. Wireless Sensor Network Security: A Survey. – In: Y. Xiao, Ed. Security in Distributed, Grid and Pervasive Computing. CRC Press, 2006, pp. 367-405.

10. D e n e r, M. Security Analysis in Wireless Sensor Networks. – International Journal of Distributed Sensor Networks, Vol. **2014**, pp. 1-9.
11. L o p e z, J., R. R o m a n, C. A l c a r a z. Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks. – In: A. Aldini, G. Barthe, R. Gorrieri, Eds. Foundations of Security Analysis and Design V. Lecture Notes in Computer Science. Vol. **5705**. Berlin, Springer, 2009, pp. 289-338.
12. Z h a n g, X., B. K i n g. Modeling RFID Security. – In: D. Feng, D. Lin, M. Yung, Eds. Information Security and Cryptology. CISC. Lecture Notes in Computer Science. Vol. **3822**. Berlin, Springer, 2005, pp. 75-90.
13. A l g h a z z a w i, D. M. Operational and Security Requirements for RFID System. – Journal of Global Research in Computer Science, Vol. **2**, 2011, No 12, pp. 6-11.
14. T a n, C. C., J. W u. Security in RFID Networks and Communications. – In: L. Chen, J. Ji, Z. Zhang, Eds. Wireless Network Security. Berlin, Springer, 2013 pp. 247-267.
15. H w a n g, M. S., C. H. W e i, C. Y. L e e. Privacy and Security Requirements for RFID Applications. – Journal of Computers, Vol. **20**, 2009, No 3, pp 55-61.
16. Z h a n g, X., B. K i n g. Security Requirements for RFID Computing Systems. – International Journal of Network Security, Vol. **6**, 2008, No 2, pp. 214-226.
17. K n o s p e, H., H. P o h l. RFID Security. – Information Security Technical Report, Vol. **9**, 2004, No 4, pp. 39-50.
18. V e d d e r, K., F. W e i c k m a n n. Smart Cards Requirements, Properties and Applications. – In: P. Horster, Ed. Chipkarten. DuD-Fachbeiträge, Vieweg+Teubner Verlag, 1998, pp. 307-331.
19. K o, H., R. D. C a y t i l e s. A Review of Smart Card Security Issues. – Journal of Security Engineering, Vol. **8**, 2011, No 3, pp. 359-370.
20. K u n d a r a p, A., A. C h h a j l a n i, R. S i n g l a, M. S a w a n t, M. D e r e, P. M a h a l l e. Security for Contactless Smart Cards Using Cryptography. – In: N. Meghanathan, S. Boumerdassi, N. Chaki, D. Nagamalai, Eds. Recent Trends in Network Security and Applications. CNSA 2010. Communications in Computer and Information Science. Vol. **89**. Berlin, Springer, 2010, pp. 558-566.
21. T u n s t a l l, M. Smart Card Security. – In: K. E. Mayes, K. Markantonakis, Eds. Smart Cards, Tokens, Security and Applications. Boston, Springer, 2008, pp. 195-228.
22. M a r k a n t o n a k i s, K., K. M a y e s, M. T u n s t a l l, D. S a u v e r o n, F. P i p e r. Smart Card Security. – In: J. Kacprzyk, Ed. Studies in Computational Intelligence (SCI). Vol. **57**. Berlin, Springer, 2007, pp. 201-234.
23. C h e l l i, K. Security Issues in Wireless Sensor Networks: Attacks and Countermeasures. – In: Proc. of World Congress on Engineering, Lecture Notes in Engineering and Computer Science, London, 2015, pp. 519-524.
24. A m e e n, M. A., J. L i u, K. K w a k. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. – Journal of Medical Systems, Vol. **36**, 2012, No 1, pp. 93-101.
25. H a r i, P. B., S. N. S i n g h. Security Issues in Wireless Sensor Networks: Current Research and Challenges. – In: Proc. of International Conference on Advances in Computing, Communication, & Automation (ICACCA'16), Dehradun, 2016, pp. 1-6.
26. T e y m o u r z a d e h, M., R. V a h e d, S. A l i b e y g i, N. D a s t a n p o r. Security in Wireless Sensor Networks: Issues and Challenges. – International Journal of Computer Networks and Communications Security, Vol. **1**, 2013, No 7, pp. 329-334.
27. H u, F., J. Z i o b r o, J. T i l l e t t, N. K. S h a r m a. Secure Wireless Sensor Networks: Problems and Solutions. – Journal of Systemics, Cybernetics and Informatics, Vol. **1**, 2003, No 4, pp. 90-100.
28. D h a k n e, A. R., P. N. C h a t u r. Detailed Survey on Attacks in Wireless Sensor Network. – In: Proc. of International Conference on Data Engineering and Communication Technology, Advances in Intelligent Systems and Computing, Singapore, 2017 pp. 319-331.
29. P a n d e, S., M. F. U n u a k h a l u e t. Privacy and Security Challenges of RFID. – In: Proc. of Information Systems Educators Conference, Texas, 2013, pp. 1-10.
30. K u l k a r n i, G., R. S h e l k e, R. S u t a r, S. M o h i t e. RFID Security Issues & Challenges. – In: Proc. of International Conference on Electronics and Communication Systems (ICECS'16), Coimbatore, 2014, pp. 1-4.

31. G u i z a n i, S. Security Applications Challenges of RFID Technology and Possible Countermeasures. – In: Proc. of International Conference on Computing, Management and Telecommunications (ComManTel'14), Da Nang, 2014, pp. 291-297.
32. K a n n o u f, N., Y. D o u z i, M. B e n a b d e l l a h, A. A z i z i. Security on RFID Technology. – In: Proc. of International Conference on Cloud Technologies and Applications, Marrakech, 2015, pp. 1-5.
33. K h a t t a b, A., Z. J e d d i, E. A m i n i, M. B a y o u m. RFID Security Threats and Basic Solutions. – In: Md. Ismail, Md. Sawan, Eds. RFID Security. Analog Circuits and Signal Processing. Springer, AG, 2017, pp. 27-41.
34. P i p p a l, R. S., C. D. J a i d h a r, S. T a p a s w i. Security Issues in Smart Card Authentication Scheme. – International Journal of Computer Theory and Engineering, Vol. **4**, 2012, No 2, pp. 206-211.
35. M a h a n t a, H. J., A. K. A z a d, A. K. K h a n. Power Analysis Attack: A Vulnerability to Smart Card Security. – In: Proc. of International Conference on Signal Processing and Communication Engineering Systems, Guntur, 2015, pp. 506-510.
36. H a n d s c h u h, H., E. T r i c h i n a. High Density Smart Cards: New Security Challenges and Applications. – In: Proc. of Highlights of the Information Security Solutions Europe/SECURE 2007 Conference, Europe, 2007, pp 251-259.
37. D e l f s, H., H. K n e b l. Introduction to Cryptography. Chapter 2 – Symmetric-Key Cryptography. Berlin, Springer, 2015, pp. 11-48.
38. W a r d l a w, W. P. The RSA Public Key Cryptosystem. – In: D. Joyner, Ed. Coding Theory and Cryptography. Berlin, Springer, 2000, pp. 101-123.
39. J a o, D. Elliptic Curve Cryptography. – In: P. Stavroulakis, M. Stamp, Eds. Handbook of Information and Communication Security. Berlin, Springer, 2010, pp. 35-57.
40. D í a z, R. D., V. G. M a r t í n e z, L. H. E n c i n a s, A. M. M u ñ o z. A Study on the Performance of Secure Elliptic Curves for Cryptographic Purposes. – In: M. Graña, G. J. López, O. Etxaniz, Á. Herrero, H. Quintián, E. Corchado, Eds. Advances in Intelligent Systems and Computing. Vol. **527**. Berlin, Springer, 2016, pp. 658-667.
41. B o n e h, D., M. F r a n k l i n. Identity-Based Encryption from the Weil Pairing. – In: J. Kilian, Ed. Advances in Cryptology – CRYPTO'2001. Vol. **2139**. Berlin, Springer, 2001, pp. 213-229.
42. R o s l i, R., Y. M. Y u s o f f, H. H a s h i m. A Review on Pairing Based Cryptography in Wireless Sensor Networks. – In: Proc. of IEEE Symposium on Wireless Technology and Applications (ISWTA'11), Langkawi, 2011, pp. 48-51.
43. P r e n e e l, B. Cryptographic Hash Functions: Theory and Practice. – In: G. Gong, K. C. Gupta, Eds. Progress in Cryptology INDOCRYPT 2010. Lecture Notes in Computer Science. Vol. **6498**. Berlin, Springer, 2010, pp. 115-117.
44. B o g d a n o v, A., M. K n e ž e v i ć, G. L e a n d e r, D. T o z, K. V a r ı c ı, I. V e r b a u w h e d e. SPONGENT: A Lightweight Hash Function. – In: B. Preneel, T. Takagi, Eds. Cryptographic Hardware and Embedded Systems – CHES 2011. Lecture Notes in Computer Science. Vol. **6917**. Berlin, Springer, 2011, pp. 312-325.
45. B e r g e r, T. P., J. D. H a y e r, K. M a r q u e t, M. M i n i e r, G. T h o m a s. The GLUON Family: A Lightweight Hash Function Family Based on FCSRs. – In: A. Mitrokotsa, S. Vaudenay, Eds. Progress in Cryptology – AFRICACRYPT 2012. Lecture Notes in Computer Science. Vol. **7374**. Berlin, Springer, 2012, pp. 306-323.
46. G u o, J., T. P e y r i n, A. P o s c h m a n n. The PHOTON Family of Lightweight Hash Functions. – In: P. Rogaway, Ed. Advances in Cryptology – CRYPTO 2011. Lecture Notes in Computer Science. Vol. **6841**. Berlin, Springer, 2011, pp. 222-239.
47. M u k u n d a n, P. M., S. M a n a y a n k a t h, C. S r i n i v a s a n, M. S e t h u m a d h a v a n. Hash-One: A Lightweight Cryptographic Hash Function. – IET Information Security, Vol. **10**, 2016, No 5, pp. 225-231.
48. B u s s i, K., D. D e y, M. K. B i s w a s, B. K. D a s s. Neeva: A Lightweight Hash Function. – IACR Cryptology ePrint Archive, Vol. **2016**, 2016, pp. 1-14.
49. J a t o i, P. A., A. A. M e m o n, B. S. C h o w d h r y, M. G. U l l a h, S. L a t i f. An Efficient Hybrid Cryptographic Algorithm, Consuming Less Time for Exchanging Information in Wireless Sensor Networks. – Wireless Personal Communications, Vol. **85**, 2015, No 2, pp. 449-462.

50. B u r m e s t e r, M., B. D. M e d e i r o s. RFID Security: Attacks, Countermeasures and Challenges. – In: Proc. of 5th RFID Academic Convocation, RFID Journal Conference, Canada, 2007.
51. B e r n s t e i n, D. A State-of-the-Art Message-Authentication Code. – In: D. Bernstein's Webpage, 2005.
http://cr.yp.to/mac.html
52. M o e i n, S., T. A. G u l l i v e r, F. G e b a l i, A. A l k a n d a r i. Hardware Attack Mitigation Techniques Analysis. – International Journal on Cryptography and Information Security (IJCIS), Vol. **7**, 2017, No 7, pp. 9-28.
53. B a r e n g h i, A., L. B r e v e g l i e r i, I. K o r e n, D. N a c c a c h e. Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures. – Proceedings of IEEE, Vol. **100**, 2012, No 11, pp. 3056-3076.
54. B u, K., M. W e n g, Y. Z h e n g, B. X i a o, X. L i u. You Can Clone but You Cannot Hide: A Survey of Clone Prevention and Detection for RFID. – IEEE Communications Surveys & Tutorials, Vol. **19**, 2017, No 3, pp. 1682-1700.
55. K h a n, W. Z., M. N. M o h a m a d S a a d, M. Y. A a l s a l e m. Scrutinising Well-Known Countermeasures against Clone Node Attack in Mobile Wireless Sensor Networks. – International Journal of Grid and Utility Computing, Vol. **4**, 2013, No 2/3, pp. 119-127.
56. S a n t i s, A. D, C. S o r i e n t e. Modified Original Smart Cards and Smart Card Clone Countermeasures. – In: Proc. of International Conference on Computational Intelligence and Security (CIS'07), Harbin, 2007, pp. 878-882.
57. M p i t z i o p o u l o s, A., D. G a v a l a s, C. K o n s t a n t o p o u l o s, G. P a n t z i o u. A Survey on Jamming Attacks and Countermeasures in WSNs. – IEEE Communications Surveys & Tutorials, Vol. **11**, 2009, No 4, pp. 42-56.
58. J a i t l y, S., H. M a l h o t r a, B. B h u s h a n. Security Vulnerabilities and Countermeasures against Jamming Attacks in Wireless Sensor Networks: A Survey. – In: Proc. of International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, 2017, pp. 559-564.
59. L o p e z, P. P., J. C. H. C a s t r o, M. J u a n, E. T a p i a d o r, A. R i b a g o r d a. Attacking RFID Systems. – In: Y. Zhang, P. Kitsos, Eds. Wireless Networks and Mobile Communications Series: Security in RFID and Sensor Networks. CRC Press, Florida, 2009, pp. 29-48.
60. B o k s l a g, W. Reverse Engineering of RFID Devices. – CoRR, 2015, Vol. **abs/1507.02196**, pp. 1-14.
61. D a i, H., H. W a n g, H. X i a o, X. L i, Q. W a n g. On Eavesdropping Attacks in Wireless Networks. – In: Proc. of IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES'16), Paris, 2016, pp. 138-141.
62. B h a r d w a j, I., A. K u m a r, M. B a n s a l. A Review on Lightweight Cryptography Algorithms for Data Security and Authentication in IoTs. – In: Proc. of 4th International Conference on Signal Processing, Computing and Control (ISPCC'17), Solan, 2017, pp. 504-509.
63. A l o t a i b i, B., K. E l l e i t h y. A New MAC Address Spoofing Detection Technique Based on Random Forests. – Sensors, Vol. **16**, 2016, No 3, p. 281.
64. K h e m i s s a, H., D. T a n d j a o u i, S. B o u z e f r a n e. An Ultra-Lightweight Authentication Scheme for Heterogeneous Wireless Sensor Networks in the Context of Internet of Things. – In: S. Bouzefrane, S. Banerjee, F. Sailhan, S. Boumerdassi, E. Renault, Eds. Mobile, Secure, and Programmable Networking. MSPN 2017. Lecture Notes in Computer Science. Vol. **10566**. Berlin, Springer, 2017, pp. 49-62.
65. H a v e r, T. Security and Privacy in RFID Applications. Master's Thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2006.
66. W e i s, S. A. Security and Privacy in Radio-Frequency Identification Devices. Master's Thesis, Massachusetts Institute of Technology, Cambridge, 2003.
67. S h a r m a, V., M. H u s s a i n. Mitigating Replay Attack in Wireless Sensor Network Through Assortment of Packets. – In: S. Satapathy, V. Prasad, B. Rani, S. Udgata, K. Raju, Eds. Proc. of 1st International Conference on Computational Intelligence and Informatics. Advances in Intelligent Systems and Computing, Springer, Singapore. Vol. **507**. 2016, pp. 221-230.

68. W a n g, Q., T. D u n l a p, Y. C h o, G. Q u. DoS Attacks and Countermeasures on Network Devices. – In: Proc. of 26th Wireless and Optical Communication Conference (WOCC'17), Newark, 2017, pp. 1-6.
69. G a s s e n d, B., D. C l a r k e, M. V. D i j k, S. D e v a d a s. Silicon Physical Random Functions. – In: Proc. of 9th ACM Conference on Computer and Communications Security. ACM, 2002, pp. 148-160.
70. S t a n d a e r t, F. X. Introduction to Side-Channel Attacks. – In: I. M. R. Verbauwhede, Ed. Secure Integrated Circuits and Systems. Integrated Circuits and Systems. Boston, Springer, 2010, pp. 27-42.
71. K h a n, A. K., H. J. M a h a n t a. Side Channel Attacks and Their Mitigation Techniques. – In: Proc. of 1st International Conference on Automation, Control, Energy and Systems (ACES'14), Hooghy, 2014, pp. 1-4.
72. G e, Q., Y. Y a r o m, D. C o c k, G. H e i s e r. A Survey of Microarchitectural Timing Attacks and Countermeasures on Contemporary Hardware. – Journal of Cryptographic Engineering, Vol. **2018**, No 1. DOI 10.1007/s13389-016-0141-6.
73. R o h a t g i, P. Electromagnetic Attacks and Countermeasures. – In: C. K. Koc, Ed. Cryptographic Engineering. Berlin, Springer, 2009, pp. 407-430.
74. P o p p, T., E. O s w a l d, S. M a n g a r d. Power Analysis Attacks and Countermeasures. – IEEE Design & Test of Computers, Vol. **24**, 2007, No 6, pp. 535-543.
75. M a h a n t a, H. J., A. K. A z a d, A. K. K h a n. Differential Power Analysis: Attacks and Resisting Techniques. – In: J. Mandal, S. Satapathy, M. K. Sanyal, P. P. Sarkar, A. Mukhopadhyay, Eds. Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing. Vol. **340**. New Delhi, Springer, 2015, pp. 349-358.
76. D u b a i, M. J., T. R. M a h e s h, P. A. G h o s h. Design of New Security Algorithm: Using Hybrid Cryptography Architecture. – In: Proc. of 3rd International Conference on Electronics Computer Technology, Kanyakumari, 2011, pp. 99-101.
77. C h o u r a s i a, S., K. N. S i n g h. An Efficient Hybrid Encryption Technique Based on DES and RSA for Textual Data. – In: S. Satapathy, J. Mandal, S. Udgata, V. Bhateja, Eds. Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing. Vol. **433**. New Delhi, Springer, 2016, pp. 73-80.
78. P r a k a s h, S., A. R a j p u t. Hybrid Cryptography for Secure Data Communication in Wireless Sensor Networks. – In: Proc. of 2nd International Conference on Computer, Communication and Computational Sciences (RACCCS'17), Ajmer, 2017 pp 1-10.
79. R a c h m a w a t i, D., A. S h a r i f, J a y s i l e n, M. A. B u d i m a n. Hybrid Cryptosystem Using Tiny Encryption Algorithm and LUC Algorithm. – In: Proc. of 4th International Conference on Operational Research, IOP Conference Series: Materials Science and Engineering, Medan, 2018, pp 1-7.
80. Z h e n g, Y. Digital Signcryption or How to Achieve Cost(Signature Encryption) « Cost(Signature) + Cost(Encryption). – In: Proc. of 17th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'97), London, 1997, pp. 165-179.
81. C a o, Z., L. L i u. On the Disadvantages of Pairing-Based Cryptography. – IACR Cryptology e-Print Archive, Vol. **2015**, pp. 84.
82. Z h e n g, Y., H. I m a i. How to Construct Efficient Signcryption Schemes on Elliptic Curves. – Information Processing Letters, Vol. **68**, 1998, No 5, pp. 227-233.
83. H w a n g, R. J., C. H. L a i, F. F. S u. An Effcient Signcryption Scheme with Forward Secrecy Based on Elliptic Curve. – Journal of Applied Mathematics and Computation, Vol. **167**, 2005, No 2, pp. 870-881.
84. T o o r a n i, M., A. A. B. S h i r a z i. An Elliptic Curve-Based Signcryption Scheme with Forward Secrecy. – Journal of Applied Sciences, Vol. **9**, 2009, No 6, pp. 1025-1035.
85. B a l a, S., G. S h a r m a, A. K. V e r m a. An Improved Forward Secure Elliptic Curve Signcryption Key Management Scheme for Wireless Sensor Networks. – In: J. Kim, K. Y. Chung, Eds. IT Convergence and Security. Lecture Notes in Electrical Engineering. Vol. **215**. Dordrecht, Springer, 2012, pp. 141-149.
86. C h a u d h r y, S. A., M. S. F a r a s h, H. N a q v i, M. S h e r. A Secure and Efficient Authenticated Encryption for Electronic Payment Systems Using Elliptic Curve Cryptography. – Electronic Commerce Research, Vol. **16**, 2016, No 1, pp. 113-139.

87. T o o r a n i, M., A. A. B. S h i r a z i. Cryptanalysis of an Elliptic Curve-Based Signcryption Scheme. – International Journal of Network Security, Vol. **10**, 2010, No 1, pp. 51-56.
88. H a g r a s, E. A., D. E. S a i e d, H. H. A l y. A New Forward Secure Elliptic Curve Signcryption Key Management (FS-ECSKM) Scheme for Heterogeneous Wireless Sensor Networks. – International Journal of Computer Science and Technology, Vol. **2**, 2011, No 2, pp. 19-23.
89. A m o u n a s, F., H. S a d k i, E. H. E. K i n a n i. An Efficient Signcryption Scheme Based on the Elliptic Curve Discrete Logarithm Problem. – International Journal of Information & Network Security, Vol. **2**, 2013, No 3, pp. 253-259.
90. W u, F., L. X u, S. K u m a r i, X. L i, A. K. D a s, M. K. K h a n, M. K a r u p p i a h, R. B a l i y a n. A Novel and Provably Secure Authentication and Key Agreement Scheme with User Anonymity for Global Mobility Networks. – Security and Communication Networks, Vol. **9**, 2016, pp. 3527-3542.
91. C h o i, Y., D. L e e, J. K i m, J. J u n g, J. N a m, D. W o n. Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. – Sensors, Vol. **14**, 2014, pp. 10081-10106.
92. H e, D., N. K u m a r, N. C h i l a m k u r t i. A Secure Temporal-Credential-Based Mutual Authentication and Key Agreement Scheme with Pseudo Identity for Wireless Sensor Networks. – Information Sciences, Vol. **321**, 2015, pp. 263-277.
93. J i a n g, Q., S. Z e a d a l l y, J. M a, D. H e. Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks. – IEEE Access, Vol. **5**, 2017, pp. 3376-3392.
94. W a n g, C., G. X u, J. S u n. An Enhanced Three-Factor User Authentication Scheme Using Elliptic Curve Cryptosystem for Wireless Sensor Networks. – Sensors, Vol. **17**, 2017, pp. 1-20.
95. Z h a n g, K., K. X u, F. W e i. A Provably Secure Anonymous Authenticated Key Exchange Protocol Based on ECC for Wireless Sensor Networks. – Wireless Communications and Mobile Computing, Vol. **2018,** 2018, pp. 1-9.
96. L i, X., J. N i u, S. K u m a r i, F. W u, A. K. S a n g a i a h, K. R. C h o o. A Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments. – Journal of Network and Computer Applications, Vol. **103,** 2018, pp. 194-204.
97. G ó d o r, G., N. G i c z i, S. I m r e. Elliptic Curve Cryptography Based Mutual Authentication Protocol for Low Computational Capacity RFID Systems – Performance Analysis by Simulations. – In: Proc. of IEEE International Conference on Wireless Communications, Networking and Information Security, Beijing, 2010, pp. 650-657.
98. Z h a n g, X., L. L i n s e n, Y. W u, Q. Z h a n g. An ECDLP-Based Randomized Key RFID Authentication Protocol. – In: Proc. of International Conference on Network Computing and Information Security, Guilin, 2011, pp. 146-149.
99. Z h a o, Z. A Secure RFID Authentication Protocol for Healthcare Environments Using Elliptic Curve Cryptosystem. – Journal of Medical Systems, Vol. **38**, 2014, No 5, pp. 1-7.
100. L i a o, Y. P., C. M. H s i a o. A Secure ECC-Based RFID Authentication Scheme Integrated with ID-Verifier Transfer Protocol. – Ad Hoc Networks, Vol. **18**, 2014, pp. 133-146.
101. A l a m r, A. A., F. K a u s a r, J. S. K i m. Secure Mutual Authentication Protocol for RFID Based on Elliptic Curve Cryptography. – In: Proc. of International Conference on Platform Technology and Service (PlatCon), Jeju, Korea, 2016, pp. 1-7.
102. J i n, C., C. X u, X. Z h a n g, F. L i. A Secure ECC-Based RFID Mutual Authentication Protocol to Enhance Patient Medication Safety. – Journal of Medical Systems, Vol. **40**, 2015, No 1, pp. 1-6.
103. Z h e n g, L., Y. X u e, L. Z h a n g, R. Z h a n g. Mutual Authentication Protocol for RFID Based on ECC. – In: Proc. of IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, 2017, pp. 320-323.
104. D i n a r v a n d, N., H. B a r a t i. An Efficient and Secure RFID Authentication Protocol Using Elliptic Curve Cryptography. – Wireless Networks, Vol. **2017**, 2017, pp. 1-15.
105. X i e, Q., D. S. W o n g, G. W a n g, X. T a n, K. C h e n, L. F a n g. Provably Secure Dynamic ID-Based Anonymous Two-Factor Authenticated Key Exchange Protocol with Extended Security Model. – IEEE Transactions on Information Forensics and Security, Vol. **12**, 2017, No 6, pp. 1382-1392.

106. P i p p a l, R. S., C. D. J a i d h a r, S. T a p a s w i. Robust Smart Card Authentication Scheme for Multi-Server Architecture. – Wireless Personal Communications, Vol. **72**, 2013, No 1, pp. 729-745.
107. Y e h, K. H. A Provably Secure Multi-Server Based Authentication Scheme. – Wireless Personal Communications, Vol. **79**, 2014, No 3, pp. 1621-1634.
108. W a n g, D., N. W a n g, P. W a n g, S. Q i n g. Preserving Privacy for Free Efficient and Provably Secure Two-Factor Authentication Scheme with User Anonymity. – Information Sciences, Vol. **321**, 2015, pp. 162-178.
109. O d e l u, V., A. K. D a s, A. G o s w a m i. An Effective and Robust Secure Remote User Authenticated Key Agreement Scheme Using Smart Sards in Wireless Communication Systems. – Wireless Personal Communications, Vol. **84**, 2015, No 4, pp. 2571-2598.
110. C h a u d h r y, S. A., H. N a q v i, K. M a h m o o d, H. F. A h m a d, M. K. K h a n. An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography. – Wireless Personal Communications, Vol. **2016**, 2016. Doi: 10.1007/s11277-016-3745-3.
111. T r u o n g, T. T, M. T. T r a n, A. D. D u o n g, I. E c h i z e n. Provable Identity Based User Authentication Scheme on ECC in Multi-Server Environment. – Wireless Personal Communications, Vol. **95**, 2017, No 3, pp. 2785-2801.
112. Z h a o, Y., S. L i, L. J i a n g. Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment. – Security and Communication Networks, Vol. **2018**, 2018, pp. 1-13.
113. S i n g h, P., P. S h e n d e. Symmetric Key Cryptography: Current Trends. – International Journal of Computer Science and Mobile Computing, Vol. **3**, 2014, No 12, pp. 410-415.
114. M u s h t a q, M. F., S. J a m e l, A. H. D i s i n a, Z. A. P i n d a r, N. S. A. S h a k i r, M. M. D e r i s. A Survey on the Cryptographic Encryption Algorithms. – International Journal of Advanced Computer Science and Applications, Vol. **8**, 2017, No 11, pp. 333-344.
115. M i t a l i, V. K u m a r, A. S h a r m a. A Survey on Various Cryptography Techniques. – International Journal of Emerging Trends & Technology in Computer Science, Vol. **3**, 2014, No 4, pp. 307-312.
116. S i n g h, S. R., A. K. K h a n, T. S. S i n g h. A Critical Review on Elliptic Curve Cryptography. – In: Proc. of International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT'16), Pune, 2016, pp. 13-18.

Received: 07.09.2018; Second Version: 08.12.2018; Accepted: 27.12.2018