Journal of Information Security and Applications 70 (2022) 103346

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A perspective trend of hyperelliptic curve cryptosystem for lighted weighted environments

Shamsher Ullah [a,*], Zheng Jiangbin [a,*], Muhammad Tanveer Hussain [b,*], Nizamud Din [c], Farhan Ullah [a], Muhammad Umar Farooq [d]

[a] School of Software, Northwestern Polytechnical University, Xian, 710072, PR China
[b] Department of Mathematics, University of Management and Technology, Lahore, 54770, Pakistan
[c] Department of Computer Science, University of Chitral, Chitral, 17200, Pakistan
[d] Department of Electronic and Electrical Engineering, Southern University of Science and Technology, Shenzhen, 518055, PR China

ARTICLE INFO

Keywords:
Encryption
Digital signature
Discrete Logarithm Problem
Signcryption
Hyper elliptic curves
Hyper elliptic curves cryptography
Low Constrained Environments

ABSTRACT

In modern cryptography, Light Weighted Environments (LWE) refer to low-constrained environments (Pelzl et al., 2003) such as smartphones and other electronic devices (Ullah et al., 2020). There is a significant effect on user-to-user, user-to-server, server-to-user, and other forms of inter-communication due to the LWE. The researcher employs many cryptographic techniques, including encryption, decryption, signcryption, and digital signature, to heighten the effect of information security in LWE scenarios. The challenging task of the proposed techniques, such as RSA, Discrete Logarithm Problem (DLP), Elliptic Curves (EC), etc., is unsuitable for LWE. Due to the large key size, it does not provide an efficient solution in terms of computation and communication costs. Therefore, the researchers use the concept of the Hyper Elliptic Curve (HEC), which is more suitable for LWE.

In this paper, we analyze the concept of HEC for resource-constrained environments. The HEC perspective trend is used to ensure the maintenance of the security of LWE and to provide effective performance in computation and communication overheads.

1. Introduction

The goal of information security is to prevent unauthorized access to information systems. It involves preventing or reducing the potential of unauthorized access, use, exposure, disruption, erasure, distortion, change, inspection, or recording of information systems and data. If a security incident occurs, it is the role of information security specialists to reduce the negative implications. It is crucial to remember that data might be electronic or physical, concrete or intangible. Although maintaining organizational productivity is often a priority when designing an information security policy, the primary focus of any information security policy should be protecting the confidentiality, integrity, and availability of data. The researchers use cryptographic techniques to hold information security practices at the industry level. It is important to encrypt both data in transit and data at rest to protect data confidentiality and integrity. Cryptography often uses digital signatures to authenticate the data. The importance of cryptography and encryption has grown in recent years. The Advanced Encryption Standard (AES) is an excellent illustration of how cryptography. AES is a symmetric key technique used to secure sensitive government information.

Nowadays, the fast advancement of information technology and wireless networks are widely utilized to send crucial information about real-time data monitoring. It is necessary to have security systems to provide data integrity, confidentiality, and authenticity. Implementing an appropriate cryptosystem in this environment is difficult because these networks are made up of many small and smart devices that are limited in terms of memory, processing capacity, etc. To address the security risks associated with wireless sensor networks, symmetric and asymmetric methods are presented in [1–4]. This strategy either requires pre-distributed keys, which means more setup work before deployment, or it produces a large amount of traffic, which results in increased energy usage [5].

1.1. Symmetric cryptosystem

The simplest kind of encryption since it only requires a single secret key to cipher and decode the information, making it the most secure. Symmetric encryption is a well-established and well-understood method. The game utilizes a secret key, which might be a number,

* Corresponding authors.
E-mail addresses: shamsherullah@nwpu.edu.cn (S. Ullah), zhengjb@nwpu.edu.cn (Z. Jiangbin), tanveerhussain@umt.edu.pk (M.T. Hussain).

https://doi.org/10.1016/j.jisa.2022.103346

Available online 14 October 2022
2214-2126/

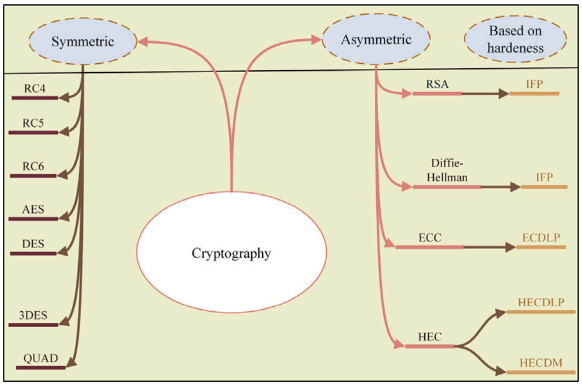

Fig. 1. General flow of the cryptographic techniques.

phrase, or string of random characters. It is used in conjunction with plain text to alter a message's content in a certain manner. There should be no knowledge of the secret key used to encode and decode all of the communications being transmitted and received by either participant. Symmetric encryption algorithms such as Blow-fish, AES, RC4, DES, RC5, and RC6 are examples. The AES (128, 192, 256) algorithms are the most commonly used symmetric algorithms.

1.2. Asymmetric cryptosystem

N. Koblitz [6] proposed the Hyperelliptic Curve Cryptosystem (HCC) based on DLP, on the Jacobian (J) of HEC over FF. The primary distinction between ECC and HECC is in group operation, which consists of various sequences of operations. The points on HEC, unlike EC, do not form a group. The divisor class group is the additive group on which the cryptographic primitives are implemented. This group's members are all decreased divisors. For implementing cryptographic primitives, HCC divisor group operations are more complicated than ECC point operations. As a result, implementing HCC in a limited context is difficult. HECC is especially relevant for secure communication in wireless sensor networks because of the restricted resources (storage, time, or power) available to sensor nodes. We can build genus 2 HECC on FF (80-bit), which provides the same degree of security as ECC (160-bit) or RSA (1024-bit). However, HEC may be used to boost security since they have certain advantages over ECC. To calculate the group operations for these curves using HECC over a Finite Field (FF), 40-bit to 80-bit long operands are required. To provide the same level of security, ECC requires operand lengths of around 160 bits, while RSA requires operand lengths of about 1024 bits. As a result, HECC is more suited for deployment on restricted platforms in wireless networks [5,7]. The user's documents must be encrypted during transmission in online banking, business networks, and other business activities. Digital signature technology should also prevent fraudulent tampering to ensure their authenticity and non-repudiation [8]. The general flow of cryptographic techniques is shown in Fig. 1.

The notation table of our paper is shown in Table 1.

1.3. Motivation

To secure data in resource-constrained networks is increasing with technological advancements. Security of transmitted information is a crucial component of any communication system. It becomes even more crucial when it comes to resource-constrained and mobile networks. Security is an application that uses a lot of energy, memory, and processing, so it is important to be mindful of this when securing resource-constrained networks. By combining digital signatures and encryption with HEC, secrecy and authenticity may be guaranteed. For networks with limited resources, HECC is the best option since it offers great efficiency and smaller key size while yet offering the same degree of security as other public key cryptosystems.

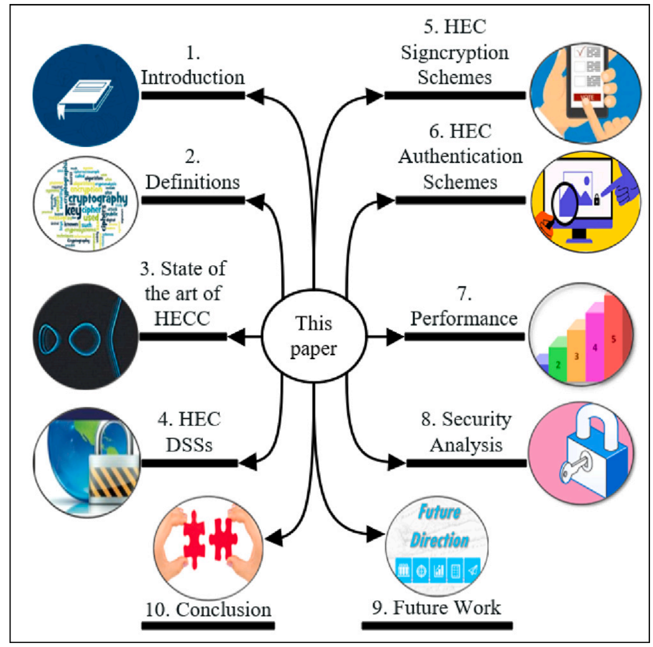

Fig. 2. The structure of the paper.

1.4. Contributions

HECC is moving from traditional academic attention to having uses in the digital world. Based on EC, the proposed methods did not catch on because they gave probabilistic results regarding computation, communication costs, and security. Due to the large key size, EC does not provide performance efficiency (high computation and communication costs). To reduce the costs and provides security, we focus on HEC for LWE. HEC over J cryptosystem is secure same as EC rational point group of the same order. HEC provides the same security level with a short key length compared to EC. The 60 bits of HEC are more secured than EC 160 bits and RSA 1024 bits. The attacks against HEC with low $4 \leq g$ demonstrate that it is incompatible with exponential complexity. HEC in the same domain cryptosystem construction is much easier for security maintenance due to the genus ($4 \leq g$).

1.5. Organization of the paper

The structure of this paper (Fig. 2), Section 3 presents the State of the art of HECC. Section 4, presents the HEC digital signature schemes (DSSs). Section 5, presents the HEC signcryption schemes. Section 6, presents the HEC authentication schemes. Sections 7 & 8 described performance and security analysis. Finally, future research direction and conclusion is presents in Sections 9 & 10 respectively.

2. Definitions

The definitions and its impacts are defined below one by one.

Definition 1 (*[9]*)**.** HEC of genus g over ϕ, if no point on the curve over the algebraic closure $\bar{\phi}$ of ϕ satisfies $2\tau_2 + h = 0$ and $f' - h'\tau_2 = 0$ (for both partial derivatives) as Eq. (1).

$$\tau : {\tau_2}^2 + h(\tau_1)\tau_2 = f(\tau_1), h, f \in \phi[\tau_1], \quad deg(f) = 2g + 1, \; deg(h).g, \; f \; monic \tag{1}$$

Table 1
Notations and their descriptions.

Symbol	Description	Symbol	Description
HECC	Hyper Elliptic Curve Cryptography	HCC	Hyperelliptic Curve Cryptosystem
DLP	Discrete Logarithm Problem	EC	Elliptic Curve
LWE	Lighted Weighted Environment	AES	Advanced Encryption Standard
FF	Finite Field	RSA	Rivest, Shamir and Adleman
J	Jacobian	NDN	Named Data Networking
DSS	Digital Signature Scheme	Ψ	Field
L	Length of the field	g	Genus
$(\mathbb{D})$	Divisor	Ω	Nontrivial Automorphism
τ	HEC	$\zeta_1,\dots,\zeta_{2g+2}$	Weierstrass Point
p	Prime	$(\bar{f}(\tau_1))$	Monic Polynomial
IFP	Integer Factorization Problem	$\mathbb{N}$	Positive Integer
(n,e)	RSA Public Key	C	Ciphertext
M	Message	η	EC
K	FF	$\mathbb{G},\mathbb{G}_\tau$	Cyclic Groups
τ	Prime Order	e	Bilinear Pairing
ROM	Random Oracle Model	1	Identity Element
ϕ	Tate-Pairing	FAG	Finite Abelian Groups
FPGA	Finite Programmable Gate Array	HDL	Hardware Description Language
DSA	Digital Signature Algorithm	ESS	Embedded System Security
XILINX	Company Name	$nuMONGO$	Library Name
D	Divisor	DS	Digital Signature
GEZEL	Design Environment	FSMD	Finite State Machine + Data-path
I/O	Input/Output	GF	Galois Field
θ	Mapping	pk	Public Key
Montgomery's REDC	Reduction Algorithm	NIST	National Institute of Standards and Technology
s_k	Private Key	σ	Blind Signature
HECDMP	HEC Divisor Multiplication Problem	BSS	Blind Signature Scheme
U_s	Senders	U_i	Signers
U_c	Signature Collector	U_v	Signature Verifier
WSN	Wireless Sensor Network	SHA	Secure Hash Algorithm
NS2	Network Simulator 2	RTL	Register Transfer Logic
PKC	Public Key Cryptography	ECDS	Elliptic Curve Digital Signature
h	Secure Small Factor	l	Large Prime Number
H	Hash Function	RFID	Radio Frequency Identification
SKC	Secret Key Cryptosystem	IoT	Internet of Things
IIoT	Industrial IoT	BAN	Body Area Network
AVISPA	Automated Validation of Internet Security Protocols and Applications	$e(a.\mathbb{R},b.\mathbb{S})=e(\mathbb{R},\mathbb{S})^{ab}$	Bilinear
WBAN	Wireless BAN	IoHT	Internet of Health Things
H/W and S/W	Hardware and Software	ICT	Information & Communication Technologies
M-Health	Mobile Health	SMH	Signcryption for Mobile Health
MBAN	Medical BAN	VANET	Vehicular Ad-hoc NETwork
RSU	Road Side Unit	ABE	Attribute Based Encryption

Definition 2 (*Jacobian* (J) *[1]*)**.** Let a field Ψ, with $F_q \subset \Psi \subset L$, the group of Ψ-rational points of the J of τ is $\tau^0\tau(\psi)/\zeta\tau(\psi)$. It is denoted by $J_\tau(\Psi)$.

Definition 3 (*HEC Divisor* ($\mathbb{D}$) *[1]*)**.** Let a divisor ($\mathbb{D}$) on HEC (τ) of g is called semi-reduced if it has the form $\mathbb{D} = \sum_{\zeta\in(\tau)} \tau\zeta([\zeta]-[\infty])$.

Definition 4 (*Andre Weil [1]*)**.** If τ is HEC over F_q of genus g, then $(\sqrt{q}-1)^{2g} \leq \#J_\tau(\psi) \leq (\sqrt{q}+1)^{2g}$.

Definition 5 (*HEC Degree 2 [9]*)**.** A non-singular curve τ/ψ of genus $g > 1$ is called HEC if $\psi(\tau)$ is a function field and has a separable extension of $degree$ 2 of the $\psi(\tau_1)$ (rational function field) for some function τ_1.

Definition 6 (*Weierstrass Points [9]*)**.** Let Ω denote the nontrivial automorphism of this extension. It induces an involution Ω^* on τ with quotient P^1. The fixed points $\zeta_1,\dots,\zeta_{2g+2}$ of Ω^* are called Weierstrass points.

Definition 7 (*Mumford Representation [9]*)**.** Let τ be a genus g HEC as in (Eq. (1)) given by $\tau : {\tau_2}^2 + h(\tau_1)\tau_2 = f(\tau_1)$, where $h, f \in \psi[\tau_1], deg\ f = 2g+1, deg\ h \leq g$.

Definition 8. Let $p \geq 3$ be a prime number and F_q a FF with $q = p^d$ elements and algebraic closure F_q [9].

Definition 9. Let $\bar{\tau}$ be a HEC [9] of genus g defined by the Eq. (2)

$$ {\tau_2}^2 = \bar{f}(\tau_1) \tag{2}$$

A monic polynomial ($\bar{f}(\tau_1)$) of degree $2g+1$.

2.1. Intractable problem

In the intractable problem, we present such types of discrete problems based on HEC.

2.1.1. Discrete logarithm problems

1. Integer Factorization Problem (IFP): IFP is an old and well-known problem. It can be defined below:

Definition 10. Let $\mathbb{N}$ is a positive integer, and to compute its decomposition into prime numbers $\mathbb{N} = \prod p_i^{e_i}$ [10].

Definition 11 (*RSA Problem [11]*)**.** Let RSA public key (n,e) and a ciphertext $C = M^e(mod\ n)$, to compute M.

2. ECDLP: Numerous cryptographic methods rely on the intractability of DLP for their security. Integer factorization and discrete logarithm methods offer less security and efficiency than ECDLP. The ECDLP has ushered in a new era of cryptographic scheme development [12].

Definition 12 (*ECDLP [13]*)**.** Let η be an EC over K. Suppose there are points $\eta_1, \eta_2 \in \eta(K)$ given such that η_1 is of prime order and $\eta_2 \in \langle \eta_1 \rangle$. Determine k such that $\eta_2 = [k]\eta_1$.

3. HEC hard problem: This is known as HEC Divisor Multiplication Problem (HECDMP). All the divisor of the different genus of the HEC is defined in Definitions 1, 2, 3 4 and 5 respectively.

2.1.2. Bi-linear pairing problems

Definition 13 (*Bilinear Pairing*)**.** Let $\mathbb{G}, \mathbb{G}_\tau$ is a cyclic groups of prime order τ, bilinear pairing can be define as $e : \mathbb{G} \times \mathbb{G} \rightarrow G_\tau$. The DLP is hard in $\mathbb{G}$. Its properties are as follows [14]:

1. Bilinear: For all $\mathbb{R}, \mathbb{S} \in \mathbb{G}$, $a, b \in Z_q^*$, $e(a.\mathbb{R}, b.\mathbb{S}) = e\mathbb{R}\ \mathbb{S}^{ab}$.
2. Non-degenerate: There exists $\mathbb{R}, \mathbb{S} \in \mathbb{G}$, such that $e\mathbb{R}\ \mathbb{S} \neq 1$. Where 1 represents an Identity element of the group $\mathbb{G}_\tau$.
3. Computable: For all $\mathbb{R}, \mathbb{S} \in \mathbb{G}$. An efficient algorithm exists to compute $e\mathbb{R}\ \mathbb{S}$.

2.2. Theorems taxonomy

The HEC theorems is define in the Theorems 2.1, and 2.2 respectively.

Theorem 2.1 (*Tate Pairing [15]*)**.** *Let $\mathbb{D} \in \mathbb{G}$ and $\mathbb{D}' \in \mathbb{G}'$. Let ϱ be an hyper elliptic net associated to $\mathbb{D}$ and $\mathbb{D}'$. The Tate-pairing of $\mathbb{D}$ and $\mathbb{D}'$ is:*

$$\phi(\mathbb{D}, \mathbb{D}') = \left(\frac{\varrho(r+1,1)\varrho(1,0)}{\varrho(r+1,0)\varrho(1,1)}\right)^{\frac{q^k-1}{r}} \tag{3}$$

Proof. Let $a, b \in \mathbb{Z}$ by using Eq. (3), we have;

$$\frac{\varrho(a+b,0)\varrho(a-b,0)}{\varrho(a,0)^2\varrho(b,0)^2} = F_g([a]\mathbb{D}, b\mathbb{D}') \tag{4}$$

Eq. (4) represents a Mumford Coordinates of $([a]\mathbb{D}, b\mathbb{D}')$ and it is an element of F_g. Now we can fix $\varrho(1,0) \in F_g$ and choose $\varrho(1,0) = 1$, then we have

$$\left(\frac{\varrho(1,0)}{\varrho(r+1,0)}\right)^{\frac{q^k-1}{r}} = 1 \tag{5}$$

Theorem 2.2. *Let $\mathbb{D} \in \mathbb{G}$ and $\mathbb{D}' \in \mathbb{G}'$. Let ϱ be an hyper elliptic net associated to $\mathbb{D}$ and $\mathbb{D}'$. To prove that $\varrho(r+1,1)$.*

Proof. Let us suppose that the distinction between the different cases such as $g \equiv 1, 2\ mod(4)$ and $g \equiv 0, 3\ mod(4)$, then we have to compute pfaffians in the coefficients of the matrix of the polynomials of degree $(m/2)$, and the determinant tool such as a polynomial degree (m). An further critical distinction between the two scenarios is that if $g \equiv 1, 2\ mod(4)$, then $\varrho(0) = 0$.

3. State of the art of HECC

To acquire an element of a Finite Abelian Group (FAG), the DLP is used to discover the integer multiplied by the base. The proposed approaches provide a variety of p_k cryptosystems in which the trapdoor function takes large multiples of a group member. The first such cryptosystem utilized a finite field's multiplicative group. Since there are particular techniques for addressing the DLP in g_2, it is essential to look at other sources of FAG. The author focuses on the situation when the ground field has g_2 since arithmetic over such fields is especially efficient. Unless the field is very big, the multiplicative group of the field does not offer safe crypto-systems [6]. There are two main accelerators of HEC, which are described one by one below:

3.1. HEC hardware accelerator

The hardware implementation of HEC is based on the following. The detailed analysis is shown in Table 2.

1. Field Programmable Gate Array (FPGA): Using FPGAs, programmers may input a logic structure that is subsequently emulated using the FPGA's huge gate array. These logic structures are built in HDL. This implementation uses Verilog, a well-known HDL. The next step was synthesizing and building the logic design for a Xilinx Virtex II FPGA using the Xilinx Integrated Software Environment. The Modeltech Microsim simulator was also used to test the concept before implementation. The application was tested on a Pentium machine using Microsoft's Visual Studio. Further results on the software implementation will be published in a future publication. Polynomial divisions in hardware take a long time. Notably, for g_2 curves, d almost always equals 1. Only when $y_1, y_2 + H$ divides both y_1 and y_2 can degree one occur.
2. HEC Unbounded Resources: If the resources are not limited, the group addition and doubling operations of HECC may be completed in 288 and 248 clock cycles, respectively, under the proposed method. A practical scenario necessitates using an architecture consisting of one inverter, one multiplier (with $D = 8$), one adder, and one squarer, which produces the optimal area-time product. Finally, the author uses registers, which revealed the need for 19 registers with 81 bits each as a consequence of his research [16].
3. Embedded System Security (ESS): The desired level of security is attained at the expense of memory capacity and processing power, both of which are limited in cost-sensitive devices like automobile systems. Security applications based on HECC can be easily accommodated using small FPGAs like the XILINX Spartan 3 devices, which take advantage of MicroBlaze specialized interfaces [17].
4. Privacy, Trust, and Control: With increasing genus, HEC, an extension of EC, needs decreasing field sizes. HEC of genus g obtained comparable security to ECC. A g_2 HECC with an operand length of 83 bits.
5. Security Issues: In virtually all contemporary communication and computer networks, security concerns are paramount. HCC has the benefit of allowing encryption with shorter operands while maintaining the same degree of security as other PKC based on the IFP (e.g. RSA) or the DLP in FF/EC. This is the first study to our knowledge that offers hardware designs for the implementation of HCC [18].
6. Algebraic Curves: It was common practice to use algebraic curves while developing and implementing asymmetric cryptosystems such as ECC and HECC. As a result, HECC offers the same degree of security as ECC when the key and operand sizes are half the size of ECC. The occupancy of the HECC area is nearly half that of the ECC [19]. The HEC addition, composition and reduction is shown in Fig. 3.

3.2. HEC software accelerator

The software implementation of HEC is based on the following. The detailed analysis is shown in Table 2.

1. $nuMONGO$ Library: EC and HEC reference implementations over prime fields are made possible by our software library $nuMONGO$, which has been intended to be efficient. The reduction technique is Montgomery's REDC function. It performs arithmetic operations in rings Z/N_Z with the odd number of members. For clarity, $nuMONGO$ uses overloaded functions statically resolved at build time and operator over-loading for I/O only. $nuMONGO$ is written in C++ to take advantage of

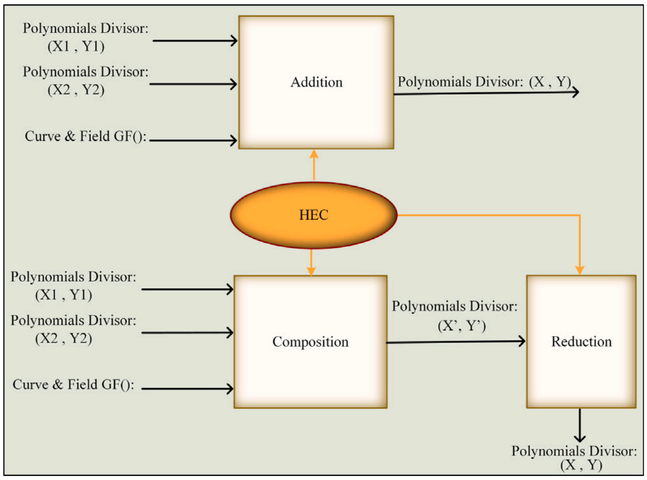

Fig. 3. HEC addition, composition and reduction.

inline functions, static resolved overloaded functions, and operator overloading for I/O only. In the C programming language, all arithmetic operations are crucial functions. $nuMONGO$ does not have any courses. All data structures are designed to be as simple as possible. All elements of Z/N_Z are stored in vectors with a fixed length of 32-bit words, which are stored in $32-bit$. Since $inlining$ has been used extensively and the majority of loops have been unrolled, there are only a few conditional branches, and as a result, branch mispredictions are uncommon. In addition to distinct arithmetic procedures for each operand size, which ranges from 32-bits to $256-bits$ in increments of $32-bits$, there are separate arithmetic routines for $48-bit$ fields [20].

2. FPGA Synthesis: For the software implementation, the authors utilized the Dalton 8051 ISS in our program, which we found to be very helpful for doing cycle-accurate simulation models, which we found to be very valuable. For the hardware/software system, the author utilized GEZEL's hardware description language to construct our co-processor multiplier, which we tested in the real world. In the explanation of the Finite State Machine+Data-path (FSMD) system modeling paradigm, one of the most important applications of the language syntax is found. It was feasible to co-simulate the 8051 with clock division circuitry using GEZEL since it interfaced with a 12 MHz hardware module in a cycle-exact way. After successfully verifying multiplier co-functionality, the processor's GEZEL code was immediately translated to RTL VHDL and loaded into Synplicity for FPGA synthesis, and implementation [21].

4. HEC DSSs

Based on the analysis, D. Jian-zhi et al. [34] banded the HECC system and DSA signature standard. The team focused on improving and analyzing the digital signature and digital validation algorithms. They incorporated HEC cryptography into the DSA algorithm and developed a digital signature system based on the HEC-DSA system. Additionally, the digital signature developed [34] may resolve the issue of determining the integrity of the file and signature ID. It is particularly well-suited for online operations that need identity validation. HECC and DSA research, HEC is transplanted into DSA, and HECDSA digital signature is created. Li-Feng Wei [35], the growth of information and network technologies has spread network communication across the production and living sectors. Network security should efficiently prevent forgery and tampering, which will apply identity authentication. Authorization and integrity of the sending file may be validated via identity authentication [36,37]. C. Yang, [38], worked on the security of digital signatures, and he describes the advantages of DLP and zero-knowledge proof protocol. He also combines the (t,n) threshold signature scheme with the participants' identities and presents DSS that relies on secret sharing. There is no trusted key distribution center in the system [38], and the secret share of the participants is created by themselves and may be utilized many times over. According to the study's results [38], the system is secure and efficient.

4.1. ElGamal signature system

It is intended for computing complexity based on the DLP and may be used for encryption and digital signature purposes. It is the second most widely used security mechanism after RSA. ElGamal system, one of the p_k encryption systems, is now being researched and used in digital signatures, electronic authentication, and security protocols, among other areas. It has been shown in prior research to have a superior encryption result than the widely used RSA algorithm.

To perform a digital signature on plaintext m using the ElGamal system, the author chooses a big prime p and creates FF for p to get a primitive root g of mode p. Select a random integer x as the private key in the field $GF(p)$ and calculate $y = g^x(mod\, p)$ as pk. The following algorithm is used to generate signatures:

1. Select k a random integer from $GF(p)$ that should be prime with p.
2. Calculate $r = g^k(mod\, p)$.
3. Find s meet the equation $s = k^{-1}(m - xr)mod\, p$.

4.2. HEC-ElGamal signature system

It was stated by Li-Feng Wei [35] that the ElGamal system is typically coupled with additional encryption techniques to create a hybrid encryption system before being used in an actual system. An HEC-Elgamal signature system is established in this design by combining the HEC and ElGamal systems in the following manner. Initially, HEC is used for message encryption, followed by the ElGamal algorithm to generate secure digital signatures for ciphertext. To combine HEC and ElGamal, the authors create one-to-one Jacobian quotient group mapping, such as $J(F_q)$ of HEC and FF $GF(p)$, $J(F_q)\ \underrightarrow{\theta(Z)}\ GF(p)$, it means to map the divisor D in group $J(F_q)$ to only integers polynomial combination in the field $GF(p)$, the mapping function of which is $\theta(Z)$.

4.3. Literature review

In the literature review, we studied all hyperelliptic curve-based schemes described one by one below.

4.3.1. DSA

The National Institute of Standards and Technology (NIST) proposed a Digital Signature Standard (DSS). The three components of DSS are the message abstract, encode, and decode. SHA produces the message abstract. Digital signatures are generated using message abstracts and have the same level of security as message abstracts [39]. Y. Lin and A. Yong-Xuan proposed a secure HEC Digital Signature Algorithm (HECDSA). They claim HECDSA is the HEC equivalent of DSA, but its security is superior. 160-bit HECDSA is nearly as secure as 1024-bit DSA. The authors also propose a generalized equation for HECDSA. These generalized signature methods may create efficient and safe cryptographic applications for many purposes. To summarize is structured as follows [40]:

(1) The HEC over FFs and their Jacobian groups are briefly described.
(2) The basic HECDSA and its three variations are given first, followed by a discussion of divisor assessments.

Table 2
HEC software & hardware accelerator on g_2.

Schemes	Tools	Hardware	Performance		
			PA	D	M
[22]	Xilinx ISE	Pentium III, 1.2 GHz	1.97 ms	1.01 ms	222 ms
[23]	Dalton 8051 ISS	GEZEL 12 MHz	11.1 ms	9.9 ms	656 ms
[16]	NTL library		288cc	248cc	–
[17]	XILINX Spartan 3	Spartan3–5000	143	104	40 ms
[24]	Verilog HDL and the Xilinx Integrated S/W Environment	Xilinx Virtex II	–	–	2.247 ms
[25]	Logic level simulation	Xilinx XC2C1000bg575–6	–	–	0.436 ms
[19]	VirtexV FPGA XC5V240	XC5V240 FPGA	0.063 ms	0.075 ms	–
[26]	ARM7	Xilnix Virtex-2 Pro	4.703 ns	4.523 ns	2.591 ns
[27]	C and compiled with GCC	Xilinx Virtex-II FPGA	–	–	0.311 ms
[28]	ARM7TDMI	P-4 processor	–	–	87.5 ms
[21]	8051 ISS	GEZEL	3.2 ms (s/w), 3.2 ms (h/w)	–	54.1 ms (s/w), 2.3 ms (h/w)
[29]	–	ARM7 (80 MHz)	0.433 ms	0.260 ms	48.35 ms
[30]	Microsoft VC++ 6.0 with inline assembler MMX and SSE2	1.6 GHz P-4	13.5 μs	13.2 μs	3.91 ms
[31]	ARMulator	ARM7TDMI	511 μs	504 μs	121.49 ms
		Pentium4@1.8 GHz	19.1 μs	18.8 μs	4.68 ms
[32]	Modelsim Simulator	Xilinx Virtex II FPGA	–	–	2.03 ms
[33]	NLT	Alpha 21 264/667 MHz	4.27 μs	4.09 μs	932 μs

Where PA stands for point addition, D for doubling, M for multiplication, cc for clock cycles, ms, ns, and μ for milli, nano, and microseconds.

(3) Two HECDSA equations and a 4-tuple HECDSA scheme are presented.
(4) In this paper, the author presented a generalized equation for HECDSA, as well as many generic HECDSA types. After that, their financial assets are scrutinized.

4.3.2. Digital Signature (DS)

A. Nelasa and T. Fedoronchak [41] worked on using HEC in the digital signature protocol. According to the mathematical basis used by A. Nelasa and T. Fedoronchak, let F be a finite field and let $\overline{F}$ be the algebraic closure of F. The HEC C of a genus $g > 1$ over the F represents a set of solutions $(x, y) \in F \times F$ the Eq. (6) is [41]:

$$C : y + h(x)y = f(x) \tag{6}$$

As a result, it is feasible to alter protocols for digital signatures on ECs by using operations with divisors on the Jacobian of an HEC as base cryptography transformations. This results in the transformation of the operations with points of EC and divisors of HEC [41]. A. Nelasa and T. Fedoronchak considered the HEC of a genus $g = 2$:

$$y^2 = x^5 + 2x^2 + x + 3 \ over\ GF_{(7)} \tag{7}$$

A. Nelasa and T. Fedoronchak [41] demonstrate that it is possible to implement a digital signature protocol based on previously introduced group divisors (Jacobian) of a higher-order HEC. To accomplish this, A. Nelasa and T. Fedoronchak modify the protocol for use over a simple field of the Galois. A. Nelasa and T. Fedoronchak concluded that a small field was chosen to demonstrate the curve. To provide a suitable degree of secrecy in the actual cryptosystem, the size of the base field is big. It was stated by S. Singh et al. [42] that digital signatures are required for secure distributed systems. G. Qiu et al. [43] have extended the Schnorr type broadcasted multi-signature to HECC, and a Schnorr type digital multi-signature scheme based on HECC has been developed. Since the HECDMP lies at the foundation of the scheme's security, it is guaranteed to be secure. The short operand and high calculating offer efficiency benefits and other advantages such as the short operand and high calculating. The Schnorr broadcasting multi-signature scheme based on the HECC comprises the selection of system settings, the signing and verifying processes, and the process of encrypting the signature. The message sender U_s, a number of signers $U_i (i = 1, 2, \dots, n)$, signature collector U_c as well as the signature verifier U_v. Y. Qing et al. [44] proposed a better digital signature method based on the elliptic curve. In addition, the security and complexity of digital signatures are discussed in detail. A digital signature method suggested by Y. Qing et al. can not only effectively withstand birthday attacks but can also enhance the security of digital signatures. The digital signature applications is shown in Table (see Table 3).

4.3.3. Proxy signatures

Y. Xiaolin et al. [8] enhance the security of proxy signatures; based on the analysis of existing proxy signature schemes, a proxy signature scheme based on HEC is proposed, and the scheme's security is analyzed. The authors [8] said that the scheme uses the proxy signature algorithm is transplanted into the HECC, and a proxy signature algorithm based on the HEC is constructed. The proxy signature based on the HECC is significantly safer than the elliptic curve and is used in e-commerce and network security.

C. Qinghua [45] explained in this article that most of the existing proxy DSSs are based on the DLP, and the large number factorization problem and their security are greatly threatened. To improve safety, after analyzing the existing schemes. C. Qinghua proposed a new proxy signature scheme that is based on HECDS. Further, in [45] analyzed the complexity and safety of the scheme. After comparison, this solution is significantly safer than the solution based on an elliptic curve. Y. Qing et al. [44] proposed proxy DSS with its security analysis. The two message recovery schemes may easily realize with low computation. Y. Qing et al. examine the proxy DSS utilizing examples.

4.3.4. Blind signature

The BSS is based on the following:

1. System setup: An arbitrary secure parameter 1^k is used as an input, while system parameters are used as outputs.
2. Blind signature generating: This includes system parameters and p_k as standard ones, a message m covertly entered by the user, and a private key s_k supplied by the signer, among other things.
3. Signature verification: It has three inputs:- system settings, pk, a message m, and a blind signature $\sigma(m)$, and it has one output: the outcome of the verification. A valid signature is indicated by "true", whereas invalid by "false" [46,47].

C. Fenglin et al. [48] analyze the Jacobian DLP about HEC and proposes a new sequential blind multisignature scheme based on HEC. The scheme meets the characteristics of sequential multi-signature and blind signature simultaneously, and its correctness, safety, and efficiency are analyzed. The scheme can be widely used in digital signature fields. F. Maosheng and H. Zhengfeng [49] designed a new blind DSS based on ECC and presented a user authentication scheme based on the blind digital signature. Y. Xiaolin et al. [50] proposed a BSS based on HEC to enhance the security of blind signatures. The authors analyze the security problem. Y. Xiaolin et al. replanting the strong blind signature algorithm based on planar affine into the HECC, then constructing a blind signature algorithm based on HEC. Moreover, authors of [50] said the Blind signature based on HEC is significantly

Table 3
Digital signature applications.

Schemes	Applications						
	Speed	Costs	Security	Non-repudiation	Imposter prevention	Time-stamp	Authenticity
[40]	×	✓	×	×	×	×	×
[41]	✓	×	×	×	×	×	×
[35]	×	×	✓	✓	×	×	✓
[42]	✓	✓	✓	✓	✓	✓	✓
[43]	✓	×	✓	×	×	×	×
[44]	×	✓	✓	×	×	×	×
[7]	×	×	✓	×	×	×	×
[38]	×	×	✓	×	×	×	×

safer than the elliptic curve and is very good in electronic voting and currency systems. C. Fenglin and H. Wanbao [51] proposed a new proxy BSS of multivariate linear transformation based on HEC. C. Fenglin and H. Wanbao analyzed the algebra basis of HEC and its Jacobin DLPs. W. Li et al. [52] proposed a bling signature method based on ECDS to address the computational cost of the current BSS. The strong blind signature was obtained by W. Li et al. by creating the signature equation and adding three random factors. Also, there is no need to find the inverse element of the multiplication, the number of multiplication operations is reduced, and the calculation speed of the algorithm is improved.

Mambo et al. [53,54] established proxy signature. In this system, an original signer delegated his signing power to another (proxy) signer, who could sign any message on behalf of the original signer. At the same time, the versifier could check and differentiate between the two. Tan et al. [54], proposed a proxy blind signature method that combines the security of both blind and proxy signature schemes. S. Pradhan [55], asymmetric curve-based cryptosystems have recently gained popularity, especially for embedded applications. EC is a subset of HEC. The size of the HEC operand is just a fraction of the size of the EC operand. HEC cryptography necessitates using a group order of at least $\approx 2^{160}$ members. In specifically, for a curve of g_2 with $p \approx 280$, the field F_q with $p \approx 2^{80}$ is required. HECC has a smaller minimum key size than ECC. In resource-constrained settings, this is preferable to ECC. G. Tao [56] used the restrictive blind signature technique and presented an efficient offline electronic cash system based on a kind of ECDS. This technique can realize the anonymity of users. It can also prevent malicious users from double-spending; because the number of operations on the elliptic curve is much smaller than that of the traditional discrete logarithm. Y. Qin and X. Wu [57] developed a new blind signature method based on HEC cryptography by including proxy signature arithmetic into HECC. Y. Qin and X. Wu analyzed the new scheme's security. The proposed scheme is to satisfy the unforgeability, undeniability, non-trail, and blindness [57].

HCC was incorporated into the construction and analysis of blind signatures by X. Zhou and X. Yang [58], and an improved BSS based on HCC was provided. In addition, the one-way trapdoor feature of the scheme is based on HECDMP. The algorithms use the many entitlements of HCC, such as its highly efficient and small key size. Using this approach, not only does the blind signature become more concise and secure, and it lowers the system overheads in terms of S/O and H/W application environment due to its design. The developing approach of the scheme, in addition, effectively implement the design concepts [58], which include minimal communication costs and system overheads. T. Gomathi et al. [59], developed HECC for use in Wireless Sensor Networks (WSNs). The HECC polynomial key generation utilizing the genus-2 curve was done. T. Gomathi et al. developed the HECC encryption and decryption algorithm. The findings of the performance analysis of HECC and ECC are presented. According to T. Gomathi et al. the new HECC system outperforms the current ECC technique. The WSN uses NS2 to implement Blind and Digital Signatures utilizing HECC. The results for both signature systems were compared using different performance measures. The key management and authentication method is a difficult problem in designing and implementing WSNs, according to T. Gomathi et al. [59]. WSNs have enormous memory storage, high computational complexity, and restricted resources. Another assertion by T. Gomathi et al. is that power consumption is a significant issue in WSN. So the suggested method [59] saves electricity in WSN.

4.3.5. Secure Hash Algorithm

The NIST uses a message to condense the standard Secure Hash Algorithm (SHA). SHA may be used to create a 160 bit message abstract from a message that is no longer than 264 bits in length.

4.3.6. HEC-DSA digital signature system

Combining DSA with other code algorithms is necessary to form a code system when creating a digital signature using the DSA algorithm. The message is coded with the help of a coding algorithm. In addition, the DSA algorithm is used to generate digital signatures for [60–62]. In the proposed scheme, the author combines the HEC with the DSA to create an HEC-DSA signature system that is both secure and reliable.

4.3.7. Synthesis and simulate

The authors of [34] utilized QuartusII 6.0 to produce RTL and simulated waveform. RTL is a chip circuit connector. It connects the modules and logic cells. The FPGA will be arranged according to the RTL.

4.3.8. Improved RSS based on HEC

X. Zhou studied ring signatures and concluded that they successfully address the issue of group management in group cryptosystems, thereby improving the efficiency of signature generation and verification. A signature method has become more important in many cases as electronic commerce has grown. However, ring signature systems are still challenging to apply widely. X. Zhou also enhanced the ring signature method using HCC to optimize the private key. Asymmetric secret parameter optimization avoids infinite security issues in a ring signature. In contrast, the suggested ring signature method requires less storage space, less bandwidth, and requires less system overhead [63].

4.3.9. HCC and its application in ring signature

Rivest, Shamir, and Tauman proposed a ring signature. An individual ring member may generate a legitimate signature in the ring's name without exposing his secrecy or personal details. The verifier cannot remove the ring signature's anonymity and has no idea who the true signer is. Various ring signature methods have been suggested. However, their implementation is challenging due to many security flaws and threats. Undue complexity in ring signature systems, such as divisor multiplication and modular exponential computing, many ring signature methods have insufficient security proofs and large key sizes [64,65].

4.4. HCC

In this section, we discussed the fundamental ideas behind HCC and the problems with existing HEC-based signatures and group signatures.

4.4.1. Basic principles of HCC

According to N. Koblitz [66], the DLP of the FF variant of the HEC was the inspiration for HECC. Small key size, efficiency, and ease of use are some of HECC's many advantages. Following are individual descriptions of the issues with a current approach known as HEC-based techniques:

- **(i)** The security level of a cryptosystem based on the HEC Jacobian group is the same as that of a cryptosystem based on the EC rational point group with the same order. The HECDMP problem, an NP ∩ co-AM issue in computational complexity theory, is used to ensure the security of the HECC.
- **(ii)** HECC can provide the same degree of security while operating with fewer operational parameters. Assuming the fundamental FF is 60 bits in the case of a three-generation HECC, the security level of HCC equals the security level of ECC with 180 bits, and it is much safer than RSA with 1024 bits.
- **(iii)** At the moment, all attack algorithms against HECC with low genus (g_4) are found to be inapplicable with exponent complexity. No effective attacking algorithms against HCC with genus lower than 4 have been discovered to be utterly irrelevant with sub-exponent complexity, indicating that the security of HECC can be relied on to be reliable.
- **(iv)** Using HCC, it is possible to build a safe Jacobian group with a big prime number order on a relatively small basic field [67] that has a large prime number order.

HEC is an algebraic curve that is an extension of the elliptic curve. The ECC is generalized in HECC. N. Koblitz [66] presented a HECC; its security relies on the DLP of HEC over FFs Jacobian on the intractability. It has comparable properties to elliptic curve cryptography and may give the group a structure similar to the elliptic curve. In comparison to the ECC, HCC offers significant benefits:

- **(1)** The established password method offers the same level of security with the same Jacobian elliptic curve group and rational points because HECC-based HECDMP security is NPco-AM in terms of computational complexity.
- **(2)** Unlike PKC, HCC uses shorter operands with the same security. The HCC genus 3 (based on FF) may give 60 bits. So the established cryptosystem with 180 bits is as secure as ECC and safer than 1024-bit RSA.
- **(3)** Consequently, the attack of low-genus HCC is based on the index of time, and losses of less than 4 did not discover the index time attack, indicating its reliability.
- **(4)** A big rational point group must be selected in order to get a larger rational point in a p_k cryptosystem. The HEC can structure a large prime number factor order Jacobian group on a relatively tiny base domain in order to obtain a larger rational point group.

N. Koblitz was the first to propose HCC as an extension of ECC. The elliptic curve cryptosystem is a natural extension of the HCC. HCC's security is also based on the HECDMP standard. Thus, for any $K \in Z_l^*$, the computation of $K = kP$ through k and P is computationally infeasible. Nevertheless, the computation of k via the HECDMP via the K and P is computationally infeasible. C. Qinghua and C. Yifei [68] presented and described a directed digital signature based on HECC. They asserted that this approach has additional benefits not previously mentioned. According to the authors, HECC is a natural extension of ECC; it is not a straightforward generalization. Also, HECC is faster than ECC and has a smaller basis field than ECC.

4.4.2. HEC based group signature

D. Chaum and E. V. Heyst proposed the concept of group signature for the first time. HEC based digital signature taxonomy is shown in Table (see Table 4). The following characteristics are included in a secure group signature:

- **(1)** Only a group member may create signatures in the group's name.
- **(2)** A valid signature receiver may validate a group signature without knowing who issued it.
- **(3)** A reputable agency can assist resolve disputes by locating the person who generated and issued the signature.

Although many alternative group signature systems have been proposed with varying characteristics, these schemes have proven inadequate for practical use. The following are some of the security risks and shortcomings associated with the methods:

- **(1)** The size of the singing group, the length of the group p_k, and the signature are dependent on the scale of the singing group.
- **(2)** In order to add or remove group members, the whole system must be reset, and the group pk, as well as the private keys of all group members, must be updated.
- **(3)** There are security risks associated with the schemes, including coalition attacks and generalized forgeries.
- **(4)** The techniques are inefficient in terms of both hardware and software implementation.

X. Zhou et al. proposed a better group signature method based on HCC owing to current group signature schemes' security flaws. The method avoids the link between pk and signature length with a group scale by blinding members' identities and producing identity certificates for each. The method fully utilizes the advantages of HCC, such as high efficiency, low key length, etc., and significantly increases H/W & S/W efficiency. Improved group signature method based on HCC [69]:

- **(1)** System Parameters: (1) Let C on F_q with g, where $g < 4$ and J is the Jacobian. Then we have $\#J(F_q) = hl$, where h is secure small factor and l is a large prime number (190 bits) q is a length of hl/g bits.
  (2) Let secure divisor P, where $d_1 \in J(F_q)$.
  (3) A secure Hash function is H, where $H : \{0,1\}^* \longrightarrow Z_n.n$, where n is the order of d_1 and $n > 190$ bits.
  (4) A p_k of signature generator is $K = kd_1$, where k is corresponding divisor k of the private key.
- **(2)** Member Registering Protocol: To join the signing group, a new member follows the protocol below.
  (1) Generates keys pair $(K_b = k_b d_1, k_b)$, and sends to K_b and ID_b to manager.
  (2) The manager randomly selects $x \in Z_l^*$ and computes $ID_c = h(x\|(ID_b)_u)d_1$ and sends to group member.
  (3) Group manager keep the record (ID_b, ID_c, x).
- **(3)** Identity Certificate Generating Protocol: The system requires each group member to provide their identification certificate, which the group manager issues.
  (1) A group manager randomly selects $y \in Z_l^*$ and computes $Y = yP \neq 0$ and $S_a = k_a h((ID_c)_u \| (Y)_u) + Y mod(l)$. (2) Sends (Y, S_a) to new member B and (K_b, ID_c, Y, S_a) is the identity of B.
- **(4)** Group Signature Generation Protocol: It is based on the following steps.
  (1) Message m and group member randomly selects $r \in Z_l^*$ and computes $R = rP \neq 0$, $s = (k_b - m(R)_u)r^{-1} mod(l)$ and $I = ID_c + ID_b + k_b K_a$.
  (2) Sends (m, s, R, I, K_b) to verifier.
- **(5)** Signature Verification Protocol: The verifier verifies that a valid member of the group signed the signature; otherwise, the signature would be rejected.
- **(6)** Anonymous Identity Notarization Protocol: It is necessary to remove the anonymity of group members before notarization in order to preserve the confidentiality of all protocols.

Table 4
HEC based digital signature taxonomy.

Schemes	Based on HEC							
	DS	DSA	SHA	SS	RS	GS	PS	BS
[34]	✓	✓	✓	✓	×	×	×	×
[63]	×	×	×	×	✓	×	×	×
[69]	×	×	×	×	×	✓	×	×
[40]	×	✓	×	×	×	×	×	×
[41]	✓	×	×	×	×	×	×	×
[48]	×	×	×	×	×	×	×	✓
[35]	✓	×	×	×	×	×	×	×
[68]	✓	×	×	×	×	×	×	×
[49]	×	×	×	×	×	×	×	✓
[50]	×	×	×	×	×	×	×	✓
[51]	×	×	×	×	×	×	×	✓
[42]	✓	×	×	×	×	×	×	×
[8]	×	×	×	×	×	×	✓	×
[45]	×	×	×	×	×	×	✓	×
[43]	✓	×	×	×	×	×	×	×
[52]	×	×	×	×	×	×	×	✓
[55]	×	×	×	×	×	×	×	✓
[56]	×	×	×	×	×	×	×	✓
[57]	×	×	×	×	×	×	×	✓
[44]	✓	×	×	×	×	×	✓	×
[58]	×	×	×	×	×	×	×	✓
[59]	✓	×	×	×	×	×	×	✓
[70]	×	×	×	×	✓	×	×	×
[38]	✓	×	×	×	×	×	×	×

Where × stands for No, √ for yes, DS for Digital signature, DSA for Digital signature algorithm, SHA for secure hash algorithm, SS for synthesis & simulate, RS for Ring signature, GS for Group Signature, PS for proxy signature, and BS for Blind Signature.

5. HEC signcryption schemes

In this section, we discussed HEC-based signcryption schemes.

Y. Zheng introduced the idea of signcryption, which combines the functions of signature and encryption in a single logical step [72]. J. Malone-Lee presented an identity-based signcryption system [73], which demonstrated the security characteristics of secrecy and unforgeability while also comparing the effectiveness of encryption and signature methods. Y. Zheng and H. Imai suggested EC-based signcryption. The scheme's contribution is efficient since signcryption saves 58% and 40% in computing and transmission costs, respectively, compared to signature and encryption methods [74].

Definition 14. Let g is the genus of the curve over FF of order q (F_q). The F_q group order for g_1 is $g.log_2 \approx 2^{160}$ and curve order for g_2 is $|F_q| \approx 2^{80}$ and for g_3 it is 54-bits [75].

Definition 15. Let the HEC field F, and its algebraic closure is $\bar{F}$. The HEC curve of $g > 1$ having the solution set $(a, b) \in F * F$. The Eq. (8) is:

$$C : a^2 + h(a)b = f(a) \tag{8}$$

where $h(a) \in F[a]$ is polynomial of degree g, and $f(a) \in F[a]$ is monic polynomial of degree $2g+1$. The Eq. (8) does not exists the solution set for $(a, b) \in \bar{F} * \bar{F}$ [76].

N. Koblitz [6] proposed that HCC recognizes DLP complexity based on a finite Abelian group. The finite Abelian group is appropriate for cryptosystems since it has the HEC Jacobian defined over FF. For DLP, the FF of the Abelian group is unsolvable, and its definition is;

Definition 16. Let HEC group points F_{qn} of the J over the curve is defined as DLP on $J(F_{qn})$ and D_1 and D_2 are two divisor over F_{qn}, and determine m, where m exists in Z, when $D_2 \in mD_1$ [6].

PKCs with high efficiency and small key size, such as HCC, are especially well-suited for deployment in an environment with limited resources due to their high efficiency and small key size. Digital signatures and encryption based on HCC ensure the secrecy and validity of information [77–87]. A signcryption scheme based on HEC saves computational, and communications costs [88]. The analysis of HEC-based scheme applications, limitations, and potential improvements are shown in Table 5.

1. HEC-based signcryption [76]: Y. Zheng introduced the idea of signcryption, which allows a single logical step to perform the tasks of signature and encryption at the same time [72]. Identity-based signcryption methods were suggested by J. Malone-Lee, the proposed scheme proves the security characteristics of secrecy and unforgeability, and it also compares with other encryption and signature schemes in terms of efficiency [73]. Y. Zheng and H. Imai developed a signcryption system based on EC technology. In terms of efficiency, the method makes a significant contribution since signcryption saves 58% and 40% in computing and transmission costs, respectively, compared to signature and encryption schemes [74].
2. Signcryption for RFID technology authentication [89]: RFID technology has grown in popularity due to its lower cost and faster processing time. Due to the reduced computing power of the RFID tag, implementing security and privacy mechanisms is a significant challenge. Previously, the researchers proposed hash-based, SKC-based, and ECC-based RFID systems as possible alternatives. However, several protocols could not meet all the security criteria, and others had a significant amount of computing overhead. The suggested system is based on 80-bit HEC, as opposed to 160-bit ECC, which provides more security and efficiency.
3. HEC-based signcryption worthiness: The low base field of HCC has proved to be a feasible alternative to conventional asymmetric cryptosystems in resource-constrained settings, making it a viable alternative to them. It ensures confidentiality, unforgeability, non-repudiation, forward secrecy, and public verifiability. However, HCC performs worse than traditional asymmetric cryptosystems. Public verifiable signcryption methods described over HECC are designed to meet all of the security criteria of signcryption while additionally providing forward secrecy and public verifiability, among other features [81].
4. Signcryption for multi-message communication: It is a good method for ensuring the security of multi-message communications by using hybrid encryption. The rapid development of internet technology necessitates the transmission of different message communications across a larger geographic area in order to improve heterogeneous system security [82].
5. Signcryption for Industrial Internet of Things (IIoT): IIoT is a new type of IoT, that allows sensors to work together with various smart devices to monitor machine condition, the environment, and gather data from industrial equipment. Furthermore, the low-resource device-friendly and safe scheme will attract low-resource devices and will become a perk in the IoT ecosystem [90,91].
6. Signcryption for cloud computing: On-demand network access to a shared pool of configurable computing resources that can be rapidly provided and released with little or no up-front investment in IT infrastructure is referred to as a cloud computing paradigm. As a result, cloud service providers must ensure that the data they store is protected to a suitable degree of integrity. The proposed HEC-based signcryption methods save greater computing time, and communication costs than their predecessors [88].
7. Signcryption for smart grid: A smart grid is a new ecosystem that combines smart IoT devices to handle diverse energy sources while improving efficiency and dependability. Data generated by smart grid IoT devices must be stored and controlled in the

Table 5
HEC-based scheme applications, limitations, and potential improvements.

Schemes	Applications, limitations & potential improvements		
	Applications	Limitations	Potential improvements
[34]	Integrity of file and ID distinguish	Transplantation HECC into DSA	To apply HEC-DSA for LWE such as IoT
[63]	Efficiency for engineering application	Low efficiency	To improve the efficiency of group cryptosystem for LWE
[69]	Hardware and software	Changing group scale	The group signature application needs to improve
[40]	Efficient and secure variants for PCAs	Hash function attacking	To implement all the seven general HECDSA types
[41]	Stability crypto-protocols on HEC	Limited parameter	To prove the stability of crypto protocols based on HEC
[48]	Digital signature fields	Sequential blind multi-signature	Multisignature and blind signature needs to apply in social data trading [71]
[35]	HSI, IC and IA	IA	To extend the security properties
[68]	Security	Elliptic curve cryptosystems	–
[49]	Secure in theory, suitable for practice	EC cryptosystems	To implement for LWE
[50]	E-voting and currency systems	Planar affine	–
[51]	E-voting and commerce	Multivariate linear transformation	To implement for constrained devices
[42]	To identify the ownership information	Compatibility and S/W buy issue	–
[45]	Electronic commerce	HECC	Need to extend to e-voting
[43]	Offers very high security	FF	To extends the security properties
[52]	Shorten the time, accelerate the speed, better security and storage	Algorithm	To focus on storage too
[56]	Off-line e-cash	Restrictive BS technique	–
[57]	Unforgeability, undeniability, non-trail, blindness	Transplanting a proxy signature arithmetic into HECC technique	To extends the security properties
[58]	Generalized signature forging, coalition attacks by trustworthy singers and out adversaries	HCC	To find the s/w and h/w specific environment
[59]	Actively monitoring industrial processes, machine health monitoring, and so on	Genus 2 curve	To implement for LWE
[70]	Reduce storage space, communication bandwidth	HECDMP	To improve security properties
[38]	Security of DS	No trusted key distribution center	Trusted third party need to improve the whole scheme

cloud server. Signcryption with proxy re-encryption allows a semi-trusted third party to change a ciphertext encrypted for one user into another ciphertext without knowing the original message content [92].

8. Signcryption for Body Area Networks (BAN): BSNs are flourishing in the market, thanks to the increasing number of patients treated simultaneously as the comparative advancement in wireless technology. Additionally, the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool simulates the proposed system. It satisfies security properties (e.g., confidentiality, integrity, unforgeability, patient data authenticity, forward secrecy, and non-repudiation) under the Random Oracle Model (ROM). Due to the lower processing and transmission costs, this approach is more efficient and well-suited to the resource-constrained setting of BSNs, where it is more cost-effective [93].
9. Signcryption for Wireless BAN (WBAN): WBAN and the IoT have risen to prominence as promising application domains that have the potential to improve the quality of the medical system significantly. However, because of the openness of the wireless environment and the privacy of people's physiological data, WBAN [94] and IoT are vulnerable to a variety of cyber attacks. The e-care services are one such promising application domain. There is a major need for a cryptographic method that is both efficient and highly secure and that can satisfy the requirements of devices with limited resources [95].
10. Signcryption scheme for multi-factor remote users: The most important need for remote user authentication is the ability to verify the user's identity across an insecure communication route. Even though many remote user authentication methods have been suggested, the system still has significant security vulnerabilities. Dharminder et al. authentication's system, susceptible to bio-metric recognition errors, offline password guessing attacks, impersonation attacks, and replay attacks [96].
11. Signcryption for biomedical: The Internet of Health Things (IoHT) is an expanded version of the IoT that plays a prominent role in remote data exchange. These distant data sources are physiological processes such as treatment progress, patient monitoring, and consultations, among other things. A suggested Named Data Networking (NDN) based certificateless signcryption method for IoHT is presented, which uses the security hardness of the HCC to achieve high levels of security. The proposed scheme's feasibility has been shown via security analysis and comparisons with current systems. The authors conclude by examining how secure our architecture is in protecting against man-in-the-middle attacks and replay assaults, which we do using the AVISPA tool [97].
12. Signcryption for Electronic Payments (e-Payment): The increasing popularity of Information and Communication Technologies (ICT) has significantly increased the number of people who purchase products online. In traditional e-payment systems, on the other hand, privacy and data security concerns exist for the user. Therefore, a signcryption method based on HEC is suggested to decrease the scheme's computational cost. In order to verify the validity of the user, the signcryption key is generated using the user's Aadhaar number (unique identity). It is possible to apply

Table 6
The strengths and weaknesses of HEC based software/hardware.

Schemes	Proposed works	Strengths	Weaknesses
[102]	Signcryption schemes based on HEC (Improved)	Increases the efficiency of s/w & h/w applications	Missing forward secrecy & public verification properties
[79]	Signcryption with forwarding secrecy based on HECC	Make it possible to use forward secrecy & public verifiability features	The proposed method requires a zero-knowledge protocol
[81]	HECC-based public verifiable signcryption systems with forwarding secrecy	In public verifiability, validity without breaking the secrecy and knowing the receiver's private key	Public verifiability mathematical proof missing
[103]	Using sensor-based random numbers for secure signcryption based on HEC	Smart card assaults, as well as offline password guessing attempts, are not successful	The oscillators' jitter is one of the drawbacks of generating random numbers
[104]	HEC based signcryption implementation	HEC Implementation	The implementation for constrained environments is missing such as smartphone etc
[105]	Efficient HEC-based signcryption schemes	The proposed approach reduces computational and communication expenses by up to 40%	Lacking of forwarding secrecy and integrity
[77]	Efficient and provides forward secrecy and public verifiability	The designed methodology reduces computation time by 50% & communication expenses by 30%–49%	The obligation to develop for light-weight contexts such as smart cards or mobile devices

the suggested signcryption method in real-time applications to guarantee secrecy, privacy, validity, and integrity [98].

13. Signcryption for Mobile Health (SMH): M-Health systems are a remote version of WBAN that may be used to gather patient health data in real-time using mobile devices and storing it on network servers. They are becoming more popular. Several methods and technologies may be used to obtain the data, which physicians can use to monitor, diagnose, and treat their patients.
14. Signcryption for resources-constrained devices: The IoT has become a part of our everyday lives as more and more gadgets connect to the internet, and the number of connected devices is growing at an alarming rate. Signcryption, in conjunction with the HEC, has the potential to lower the computational cost of encryption systems while also providing better security [99].
15. Signcryption for user authentication: Wireless communication systems are becoming more widespread, making them susceptible to various security threats. A large number of cryptographic methods have been suggested in order to offer high levels of security. Signcryption schemes, as a result, are beneficial in decreasing computational costs; nevertheless, they are not practical in resource-constrained settings. Because most of the previous methods were based on El-Gamal, bilinear pairing, RSA, and ECC, they were considered secure. The approach's security, on the other hand, is verified using an automated protocol validation tool [100], known as AVISPA [101]. HEC-based software/hardware strengths and weaknesses are shown in Table (see Table 6).

6. HEC authentication schemes

In this section, we discussed the HEC-based authentication schemes.

HEC is an excellent choice for secure communication in wireless networks for constrained devices. A proposed mutual authentication system based on HECDSA for safe access in limited devices. This protocol enables both entities to check the authenticity of the other entity, which is useful for constrained devices. Since the timings of our signature creation and verification are comparable to those of ECC protocol duration accessible in current literature, it can be concluded that the proposed protocol of HECC is efficient in this regard. HECC (g_2) with 80-bit operand lengths provides the same degree of security as ECC with 160-bit operand lengths. The authors believe that HECC is better for implementation on restricted platforms such as wireless networks [5].

An integrated cryptographic processor of PKC for embedded devices is based on the Open-SSL library. The architecture is intended for high-performance computing applications in the automobile industry. It is possible to modify HCC-based authentication protocols for access control systems and de-mobilizer applications in modern automobiles. They can increase the security level of these systems, but they do so at the expense of more computing power than is currently accessible in existing automobile platforms. Experiments have shown that a significant increase in computing speed may be obtained while maintaining a low gate count [106].

One of the essential factors to consider when building a secure Vehicular Ad-hoc NETwork (VANET) authentication. Authentication methods based on PKI and ECDSA. ECDSA suffers from overhead problems at the Road Side Unit (RSU) while extracting certificates from a trustworthy authority. The VANET employs a traditional identity-based signature method to protect the privacy and authenticate vehicle-to-vehicle communication and vehicle-to-RSU communication to function. The use of the various simulation settings compares the performance analysis of both the conventional signature method and the suggested ID-based signature technique [107].

Bio-metrics coupled with encryption may combat theoretical and real fraudulent activity in digital authentication, which can be very difficult to detect. It has been shown that bio-metric qualities improve the security of criminal investigations because of their fascinating characteristics, such as precision, stability, and uniqueness. Even though a variety of methods have been developed to achieve this goal, there are still certain restrictions, such as a longer computing time, limited precision, and maximum recognition time. Based on the HECC algorithm, an improved iris recognition method has been developed to address these difficulties [108].

The growing rate of ICT has resulted in the creation of Medical BAN (MBAN), which has the potential to enhance the quality of healthcare services. MBAN is susceptible to security risks and privacy assaults because it includes sensitive patient information and is often sent through wireless channels. It is essential to offer authentication to prevent unwanted access by intruders and maintain privacy. MBAN is made up of devices with limited resources that are used to monitor physiological states, lightweight authentication protocols [109] are required in order to minimize computing time, and transmission costs [110].

To guarantee the privacy and incorporate authentication to prevent attackers from gaining illegal access [111]. The security of authentication schemes based on HEC is shown in Table 7.

Table 7
HEC based authentication schemes security analysis.

Schemes	Attacks prevention									
	MiMA	SSA	KKA	PFS	Reply attack	KPA	HFA	Forgery attack	KPTA	CPA
[5]	√	√	√	√	√	×	×	×	×	×
[112]	×	×	×	×	×	√	√	×	×	×
[113]	×	×	×	×	√	×	×	×	×	×
[114]	×	×	×	√	√	×	×	×	×	×
[115]	×	×	√	×	√	×	×	√	×	×
[116]	√	×	×	×	√	×	×	×	×	×
[117]	×	×	×	×	√	×	×	×	√	√
[111]	√	×	×	×	√	×	×	×	×	×
[118]	×	×	√	×	×	×	×	×	×	×
[119]	×	×	×	×	×	×	×	√	√	×
[120]	×	×	×	×	√	×	×	×	×	×
[121]	√	×	√	×	×	×	×	×	×	×

Where × stands for No, √ for yes, MiMA for Man in the Middle Attack, SSA for Small Subgroup Attack, KKA for Known Key Attack, RA for Replay Attack, KPA for Known Possible Attack, HFA for Hash Function Attack, PFS for Perfect Forward Secrecy, KPTA for Known Plaintext Attack and CPA for Chosen Plaintext Attack.

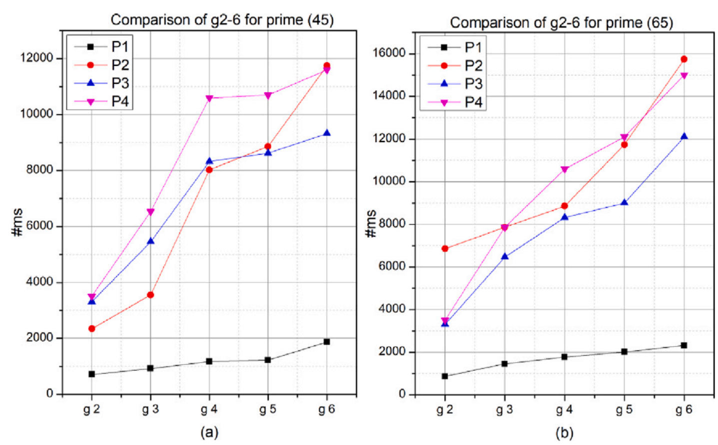

Fig. 4. Genus 2–6 processing time (ms) for length (p(45 & 65)).

7. Performance

In this section Fig. 4, shows the HEC genus (g_{2-6}) for different prime length such as 45 & 65 [122] and $P_1 \cdots P_6$ shows the processing time of the geniuses. In all geniuses, the performance ratio of the g_2 in terms of processing time is less as compared to $g_3 \cdots g_6$. As a result, HEC for embedded devices like LWE shows that digital signatures are possible within a reasonable amount of time, contrary to popular perception. The comparison of $g_2 - g_4$ HEC demonstrates that, when using the equations proposed in this work for the arithmetic on g_2 curves, the performance of g_2 and g_3 HEC across binary fields is almost similar. In virtue of the assault proposed in [123], certain curves of g_3 still perform marginally worse. It takes approximately a factor of approximately more time for g_4 curves to conduct a scalar multiple of a divisor class compared to g_2 and g_3 curves. This is because g_4 curves are substantially more complicated than g_2 and g_3 curves [29].

8. Security analysis

The data owner bears a significant amount of responsibility for the security of its customers' data. A proposed technique for efficient data security that provides secured data encryption and a protected shield against data theft is being considered for implementation. Numerous studies have focused on the statement that users, in general, must be able to access vast amounts of server data securely. However, the complexity of the cryptographic algorithm employed has not been given much consideration when it comes to security. The complexity of the algorithm has a direct impact on the speed with which data may be accessed. There is a need for an algorithm to assist us in gaining competent, quick, and secure access to data. The strong security for different cryptographic models, such as encryption, ABE, Signcryption, and Proxy Signcryption, are based on HECDMP. The computational and communication overhead is reduced due to HEC's small key size. The performance comparison of RSA, EC, and HEC is shown in Table 8.

9. Future work

HECs are a kind of algebraic curve that belongs to the class of hyperbolic curves. There are HECs for any genus $g \geq 1$ that exists. The generic formula for HEC over FF may be found here ϕ is:

$$\tau : {\tau_2}^2 + h(\tau_1)\tau_2 = f(\tau_1) \in \phi[\tau_1, \tau_2] \tag{9}$$

where $h(\tau_1), f(\tau_1) \in \phi$ satisfy certain conditions. There are two types of HEC: real and imaginary. The difference between them is the number of points at infinity.

Although Jacobian arithmetic employing imaginary models was assumed to be more straightforward and efficient than real models of HEC, their arithmetic has not been extensively researched for cryptography applications. However, recent research in this field has shown that real model arithmetic can compete with its imaginary. Real model arithmetic can take advantage of certain speedups in infrastructure scalar multiplication, which allows it to perform more quickly than its imaginary. Any method for scalar multiplication in the Jacobian may be expressed as an appropriate sequence of huge steps. The most important factor contributing to the allure of the infrastructure scenario is that, in this case, a significant number of these enormous leaps may be replaced by small steps, which are far more rapid [132].

Table 8
The security analysis of RSA, ECC and HCC.

Ref.	Environment	Contributions	Security level	Key size		
				RSA	EC	HCC
[124]	IoT and lightweight secure constrained application protocol	Transport security between IoT objects and the resource directory and achieved energy for authentication, integrity and confidentiality 75.3%, 55.7% and 47% respectively	80	1024	160–233	–
			112	2048	224–255	–
			128	3072	256–383	–
			192	7680	384–541	–
			256	15 360	512+	–
[125]	IoT high-security energy-efficient fog and mist computing devices	ECC outperforms RSA in both energy consumption and data throughput	80	1024	160–233	–
			112	2048	224–255	–
			128	3072	256–383	–
			192	7680	384–541	–
			256	15 360	512+	–
[126]	IoT elliptic curve based security for smart parking	Smart parking application domain and to protects the users privacy	80	1024	160–233	–
			112	2048	224–255	–
			128	3072	256–383	–
			192	7680	384–541	–
			256	15 360	512+	–
[127]	Embedded systems characteristics, security issues and threat model	ECC is best suited for resource constrained real time embedded systems in IoT	80	1024	160–233	–
			112	2048	224–255	–
			128	3072	256–383	–
			192	7680	384–541	–
			256	15 360	512+	–
[128]	ECC and RSA algorithm in resource constrained devices	ECC needs continues enhancement to satisfy the limitations of newly designed chips	80	1024	160–233	–
			112	2048	224–255	–
			128	3072	256–383	–
			192	7680	384–541	–
			256	15 360	512+	–
[129]	HEC on embedded systems	HEC are particularly well suited for embedded processors which are typically computationally constrained	–	–	$\approx 2^{160}$	$\approx 2^{80}$
[130]	Enhancing the security and efficiency of resource constraint devices in IoT	The implementation of zero knowledge proof with HCC enhances the security and efficiency in the resource constraint devices	256	–	94	47
			512	–	128	64
			1024	–	174	87
			4096	–	313	157
			8192	–	417	209
[131]	ECC for real time embedded systems in IoT networks	ECC is best suited for resource constrained real time embedded systems in IoT	0	1024	160–233	–
			112	2048	224–255	–
			128	3072	256–383	–
			192	7680	384–541	–
			256	15 360	512+	–

In the future, it is openly challenging for researchers to avoid the real numbers and FFs from the base of HEC schemes and replace it with complex-to-complex, real-to-complex, and complex-to-real.

1. Real HEC (RHEC): A RHEC of genus g over ϕ is defined by an equation of the form $\tau : {\tau_2}^2 + h(\tau_1)\tau_2 = f(\tau_1)$, where $h(\tau_1) \in \phi$ has degree not larger than $g+1$ while $f(\tau_1) \in \phi$ must have degree $2g+1$ *or* 2. Also, we can take q as an odd and f is a monic function. The degree of f is define as $deg(f) = 2g+2$. If q is even, then h is monic and it is define as $deg(h) = g+1$, $deg(f) \leq 2g+2$. The co-efficient is define as $x^{2g+2} \in f$, to satisfied the form of $S^2 + s$, where $s \in F_q$ [80]. RHEC $\tau : {\tau_2}^2 + h(\tau_1)\tau_2 = f(\tau_1)$ of genus g with a ramified ϕ-rational finite point $\zeta = (\zeta_1, \zeta_2)$ is birationally equivalent to a complex model $\tau' : {\tau_2'}^2 + \bar{h}({\tau_1}'){\tau_2}' = \bar{f}({\tau_1}')$ of genus g, i.e. $\deg(\bar{f}) = 2g+1$ and the function fields are equal $\phi(\tau) = \phi(\tau')$.
2. Complex HEC (CHEC): Let τ be a real quadratic curve over a field. If a ramified prime divisor of degree 1 in ϕ exists, then we can perform a bi-rational transformation to a complex quadratic curve. If a finite/infinite point equals its opposite, it is said to be ramified. It means that $\zeta = (\zeta_1, \zeta_2) = \bar{\zeta} = (\zeta_1, -\zeta_2 - h(\zeta_1))$, i.e. that $h(\zeta_1) + 2\zeta_2 = 0$. If ζ is ramified then $\zeta' = \zeta - \infty_1$ is a ramified prime divisor. HEC over FFs means that the point for complex quadratic fields there is just one absolute value (the complex one) extending Archimedes one on the base field $\mathbb{Q}$ (the real one), while for a real quadratic field is 2.

3. HEC implementation: In the future, we will implement HEC on FPGA in terms of security maintenance and efficient performance.
4. HEC security verification protocols: In the future, we will be verifying all HEC security protocols on FPGA/LWE in terms of security and privacy maintenance.

The main distinction between the real and imaginary models. The real model has two points at infinity, while the imaginary has only one point (point-of-infinity). The security of complex-to-complex, real-to-complex, and complex-to-real is hard as compared to existing schemes (real-to-real).

10. Conclusion

Today's digital world is built on a Light Weighted Environments (LWE), making it easier to navigate. The LWE significantly influences information security (users, servers or cloud, etc.). The researcher uses a variety of information security methods in order to enhance the effect of information security in LWE environments. These include encryption, decryption, signcryption, digital signature, etc. It involved bilinear pairing, DLP, and ECC, are inappropriate for LWE and does not provide an economical solution in terms of overheads and performance.

As a result, the researchers use different notions of HEC, which they believe are best appropriate for LWE. The primary focus of any information security management system should be the protection of confidentiality, integrity, and availability of data, even though maintaining organizational productivity is often a priority when establishing an information security program based on HEC.

In this paper, we analyze the concept of HEC for resource-constrained environments. HEC perspective trend is used to ensure the maintenance of security of LWE and to provide cost-effective performance in terms of computation and communication overheads.

CRediT authorship contribution statement

Nizamud Din: Conceived of the presented idea. **Farhan Ullah:** Encouraged S. Ullah for the whole manuscript. **Muhammad Umar Farooq:** Encouraged S. Ullah for the whole manuscript.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] Scholten J, Vercauteren F. An introduction to elliptic and hyperelliptic curve cryptography and the NTRU cryptosystem. In: State of the art in applied cryptography, COSIC, Vol. 3. Citeseer; 2003.
[2] Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks. In: Proceedings of the 9th ACM conference on computer and communications security. 2002, p. 41–7.
[3] Landstra T, Zawodniok M, Jagannathan S. Energy-efficient hybrid key management protocol for wireless sensor networks. In: 32nd IEEE conference on local computer networks (LCN 2007). IEEE; 2007, p. 1009–16.
[4] Watro R, Kong D, Cuti S-f, Gardiner C, Lynn C, Kruus P. TinyPK: securing sensor networks with public key technology. In: Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks. 2004, p. 59–64.
[5] Chatterjee K, De A, Gupta D. Mutual authentication protocol using hyperelliptic curve cryptosystem in constrained devices. IJ Netw Secur 2013;15(1):9–15.
[6] Koblitz N. Hyperelliptic cryptosystems. J Cryptol 1989;1(3):139–50.
[7] Fernàndez-València R. Undeniable signatures based on isogenies of supersingular hyperelliptic curves. 2019, arXiv preprint arXiv:1908.07458.
[8] Yi X-l, Zhou W, Zhao L, Jin Y-y. A proxy signature scheme based on hyperelliptic curve. J Beijing Univ Technol 2009;8.
[9] Cohen H, Frey G, Avanzi R, Doche C, Lange T, Nguyen K, Vercauteren F. Handbook of elliptic and hyperelliptic curve cryptography. CRC Press; 2005.
[10] Gaudry P. Integer factorization and discrete logarithm problems. Les Cours CIRM 2014;4(1):1–20.
[11] Rivest RL. RSA problem. MIT Laboratory for Computer Science and Burt Kaliski, RSA Laboratories; 2004, p. 1–10.
[12] Tahat N, Abdallah EE. A new signing algorithm based on elliptic curve discrete logarithms and quadratic residue problems. Ital J Pure Appl Math 2014;32(1):125–32.
[13] Lauter KE, Stange KE. The elliptic curve discrete logarithm problem and equivalent hard problems for elliptic divisibility sequences. In: Selected areas in cryptography. 2009, p. 309–27.
[14] Xiangjun X, Hailiang S. Digital signature scheme based on the inverse bilinear pairing operation problem. In: 2009 WASE international conference on information engineering, Vol. 2. 2009, p. 225–8.
[15] Tran C. Formulae for computation of tate pairing on hyperelliptic curve using hyperelliptic nets. In: International conference on cryptology in Africa. Springer; 2014, p. 199–214.
[16] Bertoni G, Breveglieri L, Wollinger T, Paar C. Finding optimum parallel coprocessor design for genus 2 hyperelliptic curve cryptosystems. In: International conference on information technology: Coding and computing, 2004. Proceedings. ITCC 2004. Vol. 2. IEEE; 2004, p. 538–44.
[17] Klimm A, Sander O, Becker J. A microblaze specific co-processor for real-time hyperelliptic curve cryptography on xilinx fpgas. In: 2009 IEEE international symposium on parallel & distributed processing. IEEE; 2009, p. 1–8.
[18] Wollinger T, Paar C. Hardware architectures proposed for cryptosystems based on hyperelliptic curves. In: 9th international conference on electronics, circuits and systems, Vol. 3. IEEE; 2002, p. 1159–62.
[19] Sghaier A, Massoud C, Zeghid M, Machhout M. Flexible hardware implementation of hyperelliptic curves cryptosystem. Int J Comput Sci Inf Secur (IJCSIS) 2016;14(4).
[20] Avanzi RM. Aspects of hyperelliptic curves over large prime fields in software implementations. In: International workshop on cryptographic hardware and embedded systems. Springer; 2004, p. 148–62.
[21] Batina L, Hwang D, Hodjat A, Preneel B, Verbauwhede I. Hardware/software co-design for Hyperelliptic Curve Cryptography (HECC) on the 8051 μP. In: International workshop on cryptographic hardware and embedded systems. Springer; 2005, p. 106–18.
[22] Boston N, Clancy T, Liow Y, Webster J. Genus two hyperelliptic curve coprocessor. In: International workshop on cryptographic hardware and embedded systems. Springer; 2002, p. 400–14.
[23] Hodjat A, Hwang D, Batina L, Verbauwhede I. A hyperelliptic curve crypto coprocessor for an 8051 microcontroller. In: IEEE workshop on signal processing systems design and implementation, 2005. IEEE; 2005, p. 93–8.
[24] Ismail MN. Towards efficient hardware implementation of elliptic and hyperelliptic curve cryptography. 2012.
[25] Kim H, Wollinger T, Choi D-H, Han D-G, Lee M-K. Hyperelliptic curve crypto-coprocessor over affine and projective coordinates. ETRI J 2008;30(3):365–76.
[26] Batina L, Mentens N, Preneel B, Verbauwhede I. Flexible hardware architectures for curve-based cryptography. In: 2006 IEEE international symposium on circuits and systems. IEEE; 2006, p. 4–pp.
[27] Fan J, Batina L, Verbauwhede I. HECC goes embedded: an area-efficient implementation of HECC. In: International workshop on selected areas in cryptography. Springer; 2008, p. 387–400.
[28] Baktir S, Pelzl J, Wollinger T, Sunar B, Paar C. Optimal tower fields for hyperelliptic curve cryptosystems. In: Conference record of the thirty-eighth asilomar conference on signals, systems and computers, 2004. Vol. 1. IEEE; 2004, p. 522–6.
[29] Pelzl J, Wollinger T, Paar C. High performance arithmetic for special hyperelliptic curve cryptosystems of genus two. In: International conference on information technology: Coding and computing, 2004. Proceedings. ITCC 2004. Vol. 2. IEEE; 2004, p. 513–7.
[30] Kitamura I, Katagi M. Efficient implementation of genus three hyperelliptic curve cryptography over GF (2n). IACR Cryptol ePrint Arch 2003;2003:248.
[31] Pelzl J, Wollinger T, Paar C. Low cost security: Explicit formulae for genus-4 hyperelliptic curves. In: International workshop on selected areas in cryptography. Springer; 2003, p. 1–16.
[32] Elias G, Miri A, Yeap T-H. On efficient implementation of FPGA-based hyperelliptic curve cryptosystems. Comput Electr Eng 2007;33(5–6):349–66.
[33] Kuroki J, Gonda M, Matsuo K, Chao J, Tsujii S. Fast genus three hyperelliptic curve cryptosystems. In: The 2002 symposium on cryptography and information security, Japan—SCIS 2002. Citeseer; 2002.
[34] Jian-zhi D, Xiao-hui C, Qiong G. Design of hyper elliptic curve digital signature. In: 2009 international conference on information technology and computer science, Vol. 2. IEEE; 2009, p. 45–7.

[35] Wei L-f. Design of hyperelliptic curve system digital signature in identity authentication. In: Fifth international conference on digital image processing (ICDIP 2013), Vol. 8878. International Society for Optics and Photonics; 2013, p. 88780X.

[36] Galbraith S. Super-singular curves in cryptography. In: Advances in cryptology Asia crypt 200. LNCS (2248), p. 495–513.

[37] Gonda M, Matsuo K, Aoki K, Chao J, Tsujii S. Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementation. IEICE Trans Fundam Electron Commun Comput Sci 2005;88(1):89–96.

[38] Yang C. Digital signature scheme based on secret sharing. J Chongqing Univ Posts Telecommun (Nat Sci Ed) 2015;27(3):418–21.

[39] Mao W. Modern cryptography. In: Theory and practice. Pearson Education; 2004, p. 184–90.

[40] Lin Y, Sang Y-X. Effective generalized equations of secure hyperelliptic curve digital signature algorithms. J China Univ Posts Telecommun 2010;17(2):100–15.

[41] Nelasa A, Fedoronchak T. Usage of hyperelliptic curves in the digital signature protocol. In: 2006 international conference-modern problems of radio engineering, telecommunications, and computer science. IEEE; 2006, p. 51–3.

[42] Singh S, Iqbal MS, Jaiswal A. Survey on techniques developed using digital signature: public key cryptography. Int J Comput Appl 2015;117(16).

[43] Qiu G, Wang X, Zhang Y. A schnorr multiple digital signatures based on the hyperelliptic curve cryptosystem. In: Proceedings of the 2015 international conference on applied mechanics, mechatronics and intelligent systems (AMMIS2015). World Scientific; 2016, p. 574–80.

[44] Yang Q, Xin X-l, Ji W. Digital signature and proxy digital signature based on elliptic curve. Comput Eng 2008;23.

[45] Qing-hua C. A proxy signature scheme based on hyper elliptic curve cryptosystems. Comput Technol Dev 2010;7.

[46] Avanzi RM. Aspects of hyper-elliptic curves over large prime fields in software implementations. In: International association for cryptology research 2004. Berlin, Heidelberg, New York: Springer-Verlag; 2004, p. 148–62.

[47] Li H-X, Cheng C-T, Pang L-J. A new (t, n)-threshold multi-secret sharing scheme. In: CIS2005. Berlin, Heidelberg, New York: Springer-Verlag; 2005, p. 421–6.

[48] Chen F-L, Hu W-B, Sun G-R. Sequential blind multisignature based on hyperelliptic curve. Comput Eng 2011;9.

[49] Chen Y-c, Zhu Y-q. A blind digital signature scheme based on hyperelliptic curve cryptosystem. Microelectron Comput 2007;11.

[50] Yi X-l, Zhou W, Lu P-c. A blind signature scheme based on hyperelliptic curve. J Beijing Univ Technol 2010;2.

[51] Chen F-l, Hu W-b. Proxy blind signature scheme based on hyperelliptic curve. J Comput Appl 2010;5.

[52] Wan L, Li F-W, Yan S-J. Blind signature scheme based on improved elliptic curve digital signature algorithm. Jisuanji Yingyong Yanjiu 2011;28(3):1152–4.

[53] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation. In: Proceedings of the 3rd ACM conference on computer and communications security. 1996, p. 48–57.

[54] Kim S, Park S, Won D. Proxy signatures, revisited. In: International conference on information and communications security. Springer; 1997, p. 223–32.

[55] Pradhan S. Proxy blind signature using hyperelliptic curve cryptography (Ph.D. thesis), 2013.

[56] Guo T, Li Z-t, Peng J-f, Wu S-z. Blind signature and off-line e-cash system based on elliptic curve. J-China Inst Commun 2003;24(9):142–6.

[57] Qin Y, Wu X. New blind signature scheme based on hyperelliptic curve. In: 2012 2nd international conference on consumer electronics, communications and networks (CECNet). IEEE; 2012, p. 400–3.

[58] Zhou X, Yang X. Hyper-elliptic curves cryptosystem based blind signature. In: 2009 Pacific-Asia conference on knowledge engineering and software engineering. IEEE; 2009, p. 186–9.

[59] Gomathi T, Manju V, Anuradha N. AN efficient blind signature authentication for wireless sensor networks using HECC. Int J Innov Sci Res 2014;10(1):6–10.

[60] Kim H, Wollinger T. Hyperelliptic curve coprocessors on FPGA. 2005.

[61] Grace Elias AM, Yeap TH. High-performance, FPGA based hyperelliptic curve cryptosystem. 2007.

[62] Jian-Zhi D. The research on digital signature based on hyper elliptic curve.

[63] Zhou X. Improved ring signature scheme based on hyper-elliptic curves. In: 2009 second international conference on future information technology and management engineering. IEEE; 2009, p. 373–6.

[64] Nakanishi T, Tao M, Sugiyama Y. A group signature scheme committing the group. In: ICICS2002. Berlin, Heidelberg, New York: Springer-Verlag; 2002, p. 73–84.

[65] Lei C. Research on anonymous fingerprinting and application to anonymity technology. Xi'an: Xidian University; 2005.

[66] Koblitz N. Hyperelliptic cryptography. J Cryptol 1989;1(3):139–50.

[67] Pfitzmann B, Waidner M. Anonymous fingerprinting. In: Advances in cryptology-EUROCRYPT'97. Berlin, Heidelberg, New York: Springer-Verlag; 1997, p. 88–102.

[68] Cai Q-h, Cheng Y-f. A directed digital signature based on HECC. Comput Technol Dev 2006;1.

[69] Zhou X, Yang X, Wei P. Hyper-elliptic curves based group signature. In: 2009 Chinese control and decision conference. IEEE; 2009, p. 2280–4.

[70] Zhou X. Hyper-elliptic curves based ring signature. In: 2009 third international symposium on intelligent information technology application, Vol. 3. IEEE; 2009, p. 674–7.

[71] Ullah S, Zhang L, Sardar MW, Hussain MT. τ-Access policy: Attribute-based encryption scheme for social network based data trading. China Commun 2021;18(8):183–98.

[72] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption)<< cost (signature) + cost (encryption). In: Annual international cryptology conference. Springer; 1997, p. 165–79.

[73] Malone-Lee J. Identity-based signcryption. IACR Cryptol ePrint Arch 2002;2002:98.

[74] Zheng Y, Imai H. How to construct efficient signcryption schemes on elliptic curves. Inform Process Lett 1998;68(5):227–33.

[75] Koblitz N. A family of jacobians suitable for discrete log cryptosystems. In: Conference on the theory and application of cryptography. Springer; 1988, p. 94–9.

[76] Ullah S, Li X-Y, Zhang L. A review of signcryption schemes based on hyper elliptic curve. In: 2017 3rd international conference on big data computing and communications. BIGCOM, IEEE; 2017, p. 51–8.

[77] Ch SA, Sher M, Ghani A, Naqvi H, Irshad A, et al. An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. Multimedia Tools Appl 2015;74(5):1711–23.

[78] Ch SA, Nasar W, Javaid Q, et al. Efficient signcryption schemes based on hyperelliptic curve cryptosystem. In: 2011 7th international conference on emerging technologies. IEEE; 2011, p. 1–4.

[79] Ch SA, Amin N, et al. Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem. In: 8th international conference on high-capacity optical networks and emerging technologies. IEEE; 2011, p. 244–7.

[80] Ullah S, Din N. Blind signcryption scheme based on hyper elliptic curves cryptosystem. Peer-to-Peer Netw Appl 2021;14(2):917–32.

[81] Ch SA, Sher M, et al. Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem. In: International conference on information systems, technology and management. Springer; 2012, p. 135–42.

[82] Rahman A, Ullah I, Naeem M, Anwar R, Khattak H, Ullah S. A lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on hyper elliptic curve. Int J Adv Comput Sci Appl 2018;9(5):160–7.

[83] Ch SA, Sher M, Ghani A, Naqvi H, Irshad A, et al. An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography. Multimedia Tools Appl 2015;74(5):1711–23.

[84] Ullah S, Junaid M, Habib F, et al. A novel proxy blind signcryption scheme based on hyper elliptic curve. In: 2016 12th international conference on natural computation, fuzzy systems and knowledge discovery (ICNC-FSKD). IEEE; 2016, p. 1964–8.

[85] Ullah Z, Ullah I, Khan H, Khattak H, Ullah S. Secure protocol for mobile agents using proxy signcryption scheme based on hyper elliptic curve. Int J Comput Sci Inf Secur 2016;14(12):1009.

[86] Ullah S, Li X-Y, Lan Z. A novel trusted third party based signcryption scheme. Multimedia Tools Appl 2020;79(31):22749–69.

[87] Pelzl J, Wollinger TJ, Guajardo J, Paar C. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves (update). IACR Cryptol ePrint Arch 2003;2003:26.

[88] Akintoye SB, Akintoye KA. Data security scheme for cloud computing using signcryption based on hyperelliptic curves. J Res Dev 2015;187(2145):1–10.

[89] Ali U, Idris MYIB, Ayub MNB, Ullah I, Ali I, Nandy T, Yahuza M, Khan N. RFID authentication scheme based on hyperelliptic curve signcryption. IEEE Access 2021;9:49942–59.

[90] Ullah I, Ul Amin N, Zareei M, Zeb A, Khattak H, Khan A, Goudarzi S. A lightweight and provable secured certificateless signcryption approach for crowdsourced IIoT applications. Symmetry 2019;11(11):1386.

[91] Hussain S, Ullah I, Khattak H, Khan MA, Chen C-M, Kumari S. A lightweight and provable secure identity-based generalized proxy signcryption (IBGPS) scheme for Industrial Internet of Things (IIoT). J Inf Secur Appl 2021;58:102625.

[92] Hussain S, Ullah I, Khattak H, Adnan M, Kumari S, Ullah SS, Khan MA, Khattak SJ. A lightweight and formally secure certificate based signcryption with proxy re-encryption (CBSRE) for internet of things enabled smart grid. IEEE Access 2020;8:93230–48.

[93] Iqbal J, Waheed A, Zareei M, Umar AI, Amin NU, Aldosary A, Mohamed EM. A lightweight and secure attribute-based multi receiver generalized signcryption scheme for body sensor networks. IEEE Access 2020;8:200283–304.

[94] Pu C, Zerkle H, Wall A, Lim S, Choo K-KR, Ahmed I. A lightweight and anonymous authentication and key agreement protocol for wireless body area networks. IEEE Internet Things J 2022.

[95] Ullah I, Alomari A, Ul Amin N, Khan MA, Khattak H. An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the Internet of Things. Electronics 2019;8(10):1171.

[96] Rajasekar V, Jayapaul P, Krishnamoorthi S. Cryptanalysis and enhancement of multi factor remote user authentication scheme based on signcryption. Adv Math Commun 2020.

[97] Ullah SS, Hussain S, Alroobaea R, Ali I, et al. Securing NDN-based internet of health things through cost-effective signcryption scheme. Wirel Commun Mob Comput 2021;2021.

[98] Devarajan M, Sasikaladevi N. A secured signcryption scheme for e-payment system using hyper elliptic curve. J Intell Fuzzy Systems 2020;(Preprint):1–11.

[99] Jadhav SP, Balabanov G, et al. Hyper-elliptic curve based signcryption schemes for resource constraint devices in IOT. Inf Technol Ind 2021;9(1):324–9.

[100] Devarajan M, Sasikaladevi N. An hyper elliptic curve based efficient signcryption scheme for user authentication. J Intell Fuzzy Systems (Preprint):1–12.

[101] Pu C, Wall A, Choo K-KR, Ahmed I, Lim S. A lightweight and privacy-preserving mutual authentication and key agreement protocol for internet of drones environment. IEEE Internet Things J 2022.

[102] Zhou XW. Improved signcryption schemes based on hyper-elliptic curves cryptosystem. In: Applied mechanics and materials, Vol. 20. Trans Tech Publ; 2010, p. 546–52.

[103] Premalatha J, Sathya K, Rajasekar V. Secure signcryption on hyperelliptic curve with sensor based random number. In: 14th international conference on recent advances on computer engineering.

[104] Kumar P, Singh A, Tyagi AD. Implementation of hyperelliptic curve based signcryption approach. Int J Sci Eng Res 2013;4(7).

[105] Din DN, Chaudhry S, Nasar W, Javaid Q. Efficient signcryption schemes based on hyperelliptic curve cryptosystem. 2011, p. 84–7. http://dx.doi.org/10.1109/ICET.2011.6048467.

[106] Klimm A, Haas M, Sander O, Becker J. A flexible integrated cryptoprocessor for authentication protocols based on hyperelliptic curve cryptography. In: 2010 international symposium on system on chip. IEEE; 2010, p. 35–42.

[107] Yadav KA, Vijayakumar P. Hyperelliptic curve cryptography-based lightweight privacy-aware secure authentication scheme for vehicular ad hoc network. In: Intelligent embedded systems. Springer; 2018, p. 83–90.

[108] Rajasekar V, Premalatha J, Sathya K. Enhanced biometric recognition for secure authentication using iris preprocessing and hyperelliptic curve cryptography. Wirel Commun Mob Comput 2020;2020.

[109] Pu C, Li Y. Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system. In: 2020 IEEE international symposium on local and metropolitan area networks (LANMAN. IEEE; 2020, p. 1–6.

[110] Sasikaladevi N, Malathi D. Energy efficient lightweight mutual authentication protocol (REAP) for MBAN based on Genus-2 hyper-elliptic curve. Wirel Pers Commun 2019;109(4):2471–88.

[111] Sasikaladevi N, Malathi D. Privacy preserving light weight authentication protocol (LEAP) for WBAN by exploring Genus-2 HEC. Multimedia Tools Appl 2019;78(13):18037–54.

[112] Kavitha S, Alphonse P, Reddy YV. An improved authentication and security on efficient generalized group key agreement using hyper elliptic curve based public key cryptography for IoT health care system. J Med Syst 2019;43(8):1–6.

[113] Ganesan SP. An authentication protocol for mobile devices using hyperelliptic curve cryptography. Int J Recent Trends Eng Technol 2010;3(2):2–4.

[114] John AL, Thampi SM. Mutual authentication based on HECC for RFID implant systems. In: International symposium on security in computing and communication. Springer; 2016, p. 18–29.

[115] Naresh VS, Reddi S, Murthy NV. Provable secure lightweight multiple shared key agreement based on hyper elliptic curve Diffie–Hellman for wireless sensor networks. Inf Secur J: Glob Perspect 2020;29(1):1–13.

[116] Chaudhry SA, Farash MS, Naqvi H, Sher M. A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. Electron Commer Res 2016;16(1):113–39.

[117] Sasikaladevi N, Geetha K, Mahalakshmi N, Archana N. SNAP-compressive lossless sensitive image authentication and protection scheme based on Genus-2 hyper elliptic curve. Multimedia Tools Appl 2019;78(18):26163–79.

[118] Kar J. Authenticated multiple key establishment protocol for wireless sensor networks. IACR Cryptol ePrint Arch 2013;2013:747.

[119] Kazmirchuk S, Anna I, Sergii I. Digital signature authentication scheme with message recovery based on the use of elliptic curves. In: International conference on computer science, engineering and education applications. Springer; 2019, p. 279–88.

[120] Devarajan M, Sasikaladevi N. An hyper elliptic curve based efficient signcryption scheme for user authentication. J Intell Fuzzy Systems (Preprint):1–12.

[121] Vijayakumar P, Vijayalakshmi V, Zayaraz G. Hybrid secure GSM architecture using DNA computing-based hyperelliptic curve cryptography. Int J Electron Secur Digit Forensics 2015;7(2):105–18.

[122] Vijayakumar P, Vijayalakshmi V, Zayaraz G. Comparative study of hyperelliptic curve cryptosystem over prime field and its survey. Int J Hybrid Inf Technol 2014;7(1):137–46.

[123] Thériault N. Index calculus attack for hyperelliptic curves of small genus. In: International conference on the theory and application of cryptology and information security. Springer; 2003, p. 75–92.

[124] Albalas F, Al-Soud M, Almomani O, Almomani A. Security-aware CoAP application layer protocol for the internet of things using elliptic-curve cryptography. Power (Mw) 2018;1333:151.

[125] Suárez-Albela M, Fraga-Lamas P, Fernández-Caramés TM. A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices. Sensors 2018;18(11):3868.

[126] Chatzigiannakis I, Vitaletti A, Pyrgelis A. A privacy-preserving smart parking system using an IoT elliptic curve based security platform. Comput Commun 2016;89–90:165–77. http://dx.doi.org/10.1016/j.comcom.2016.03.014, URL: https://www.sciencedirect.com/science/article/pii/S014036641630072X. Internet of Things Research challenges and Solutions.

[127] Dhillon PK, Kalra S. Elliptic curve cryptography for real time embedded systems in IoT networks. In: 2016 5th international conference on wireless networks and embedded systems. WECON, IEEE; 2016, p. 1–6.

[128] Bafandehkar M, Yasin SM, Mahmod R, Hanapi ZM. Comparison of ECC and RSA algorithm in resource constrained devices. In: 2013 international conference on IT convergence and security. ICITCS, IEEE; 2013, p. 1–3.

[129] Pelzl J, Wollinger T, Guajardo J, Paar C. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. In: International workshop on cryptographic hardware and embedded systems. Springer; 2003, p. 351–65.

[130] Jadhav SP, Balabanov G, Poulkov V, Shaikh JR. Enhancing the security and efficiency of resource constraint devices in IoT. In: 2020 international conference on industry 4.0 technology (I4Tech). IEEE; 2020, p. 163–6.

[131] Dhillon PK, Kalra S. Elliptic curve cryptography for real time embedded systems in IoT networks. In: 2016 5th international conference on wireless networks and embedded systems. WECON, IEEE; 2016, p. 1–6.

[132] Jacobson Jr MJ, Scheidler R, Stein A. Cryptographic aspects of real hyperelliptic curves. Cryptol ePrint Arch 2010.