information

Article

Cost-Effective Signcryption for Securing IoT: A Novel Signcryption Algorithm Based on Hyperelliptic Curves

Junaid Khan [1], Congxu Zhu [1,*], Wajid Ali [1], Muhammad Asim [2,3,*] and Sadique Ahmad [2]

[1] School of Computer Science and Engineering, Central South University, Changsha 410083, China; 214718018@csu.edu.cn (J.K.); 234708010@csu.edu.cn (W.A.)
[2] EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia; saahmad@psu.edu.sa
[3] School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China
* Correspondence: zhucx@csu.edu.cn (C.Z.); masim@psu.edu.sa (M.A.)

Abstract: Security and efficiency remain a serious concern for Internet of Things (IoT) environments due to the resource-constrained nature and wireless communication. Traditional schemes are based on the main mathematical operations, including pairing, pairing-based scalar multiplication, bilinear pairing, exponential operations, elliptic curve scalar multiplication, and point multiplication operations. These traditional operands are cost-intensive and require high computing power and bandwidth overload, thus affecting efficiency. Due to the cost-intensive nature and high resource requirements, traditional approaches are not feasible and are unsuitable for resource-limited IoT devices. Furthermore, the lack of essential security attributes in traditional schemes, such as unforgeability, public verifiability, non-repudiation, forward secrecy, and resistance to denial-of-service attacks, puts data security at high risk. To overcome these challenges, we have introduced a novel signcryption algorithm based on hyperelliptic curve divisor multiplication, which is much faster than other traditional mathematical operations. Hence, the proposed methodology is based on a hyperelliptic curve, due to which it has enhanced security with smaller key sizes that reduce computational complexity by 38.16% and communication complexity by 62.5%, providing a well-balanced solution by utilizing few resources while meeting the security and efficiency requirements of resource-constrained devices. The proposed strategy also involves formal security validation, which provides confidence for the proposed methodology in practical implementations.

Keywords: Internet of Things; security; hyperelliptic curve cryptography; discrete logarithm problem; signcryption; AVISPA

Citation: Khan, J.; Zhu, C.; Ali, W.; Asim, M.; Ahmad, S. Cost-Effective Signcryption for Securing IoT: A Novel Signcryption Algorithm Based on Hyperelliptic Curves. *Information* **2024**, *15*, 282. https://doi.org/10.3390/info15050282

Academic Editor: Zahir M. Hussain

Received: 9 April 2024
Revised: 28 April 2024
Accepted: 7 May 2024
Published: 15 May 2024

1. Introduction

The Internet of Things (IoT) is a cutting-edge technology that enables communication between real-world entities through the Internet. The primary goal of IoT technology is to enable data exchange association among the surroundings and Internet-enabled devices. The IoT architecture framework permits interactions among smart systems and physical infrastructure. The IoT framework consists of a sensing layer, network layer, and application layer [1], as shown in Figure 1.

1.1. Physical Layer

The physical/perception layer contains sensors or actuators, which are resource constraints as they have limited processing and computational power [2]. These sensors sense the physical information (physical parameters, e.g., temperature, blood pressure, humidity, etc.) by using different technologies, e.g., NFC, RFID, etc. Due to resource limitations such as device and bandwidth constraints, several security threats arise as discussed: *Denial-of-service (DoS) attack*—This can potentially block the functionality of the system

and make the network paradigm inaccessible to authorized users. Attack results can be achieved by sending spam or false flood messages, resulting in system crash or network overload and preventing accessibility to system services [3]. *Node capture*—This attack aims to compromise the IoT nodes; an adversary can easily control the network-connected nodes. Control over these nodes not only gives access to the cryptographic keys but also the protocol limitations, resulting in compromising the security of the whole network [4]. *Replay attack*—This is an attack in which valid data are intercepted and transmitted by the adversary several times without having authorization. This attack is performed against authentication protocols to steal sensitive data, and later, these data are re-transmitted to the victim [5]. *DoSL attack*—IoT networks comprise sensor nodes, which operate under certain conditions and time intervals to collect information. Due to power limitations, these nodes go to sleep to save battery life after sending the collected data. The purpose of a DoSL attack is to intensely stop the nodes from entering hibernation mode, with the aim of more power consumption and battery drainage [6]. *Side-channel attack*—The attack exploits physical system implementations and aims to gather information pertaining to hardware, power consumption, and the interference generated by the devices [7].

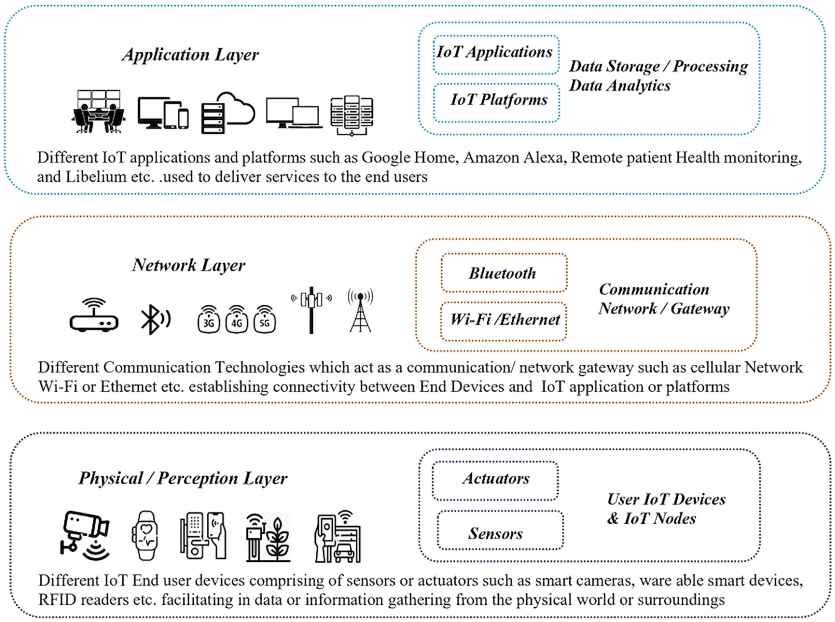

Figure 1. Overview of 3-layer IoT architecture framework.

1.2. Network Layer

The primary function of the network layer is to permit data exchange between the physical layer and the application layer. The network layer gathers data from the application layer and processes gathered data gathered to the application layer. Data are exchanged using several communication or network gateway technologies, such as LTE, Wi-Fi, Bluetooth, etc. Data management is also performed by this layer with the provision of middleware technology [8]. The network layer is vulnerable to attacks; several potential threats have been identified, and a few of them are categorized as follows: *Routing attack*—In this attack, malicious nodes disrupt the routing path by misdirecting or discarding packet forwarding by filtering any protocol information [9], e.g., a *black hole attack* [10,11]. *Grey hole attack*—This attack utilizes the weaknesses in network topological information exchange, and by using this topological knowledge, the attackers disconnect the victim from target nodes of the current network and terminate the communication services [12], e.g., *wormhole* [13] and *hello flood* [14]. Also, there are types of routing attacks [15]. *Passive attack*—A type of attack in which the intruder accesses the communication link and listens to the private communication channel, e.g., eavesdropping [16]. *Man-in-the-middle attack*—This attack takes place

when the external attacker breaches communication between two trusted entities and steals critical data [17].

1.3. Application Layer

In the IoT architecture, the application layer is positioned at the top and serves as a means to provide services to users through specialized applications. This layer holds significant importance as it facilitates the development of diverse applications utilized across various industrial and educational sectors e.g., smart cities, industry automation, agriculture, health care, and big data processing, which increases its significance [18]. The IoT framework does not adhere to any international standards; due to this, the application layer can suffer from several attacks [19]. In this layer, the attacker targets the running IoT system software, i.e., remote health monitoring software etc and gains access to the sensitive data by exploiting the software [20]. Potential attacks include *cookie hijacking*, *spyware*, *scareware*, *botnets*, *Trojan horse*, *file infection*, etc. [21].

The IoT environment faces numerous challenges in terms of security and efficiency due to limited CPU and storage resources. As a result, establishing reliable and secure communication channels becomes a major challenge for the IoT [22]. To deal with these issues, public-key cryptosystems play an important role in the IoT architecture by providing effective and secure communication by enhancing confidentiality, integrity, and authentication of transmitted data between the IoT devices.

2. Motivation and Methodology

The increasing popularity and involvement of IoT innovations in advanced technology has made them prominent in every aspect of life. However, this innovative technology faces several issues, including efficiency shortcomings and data protection. To address such challenges, the main contribution of our work is to design a lightweight and secure cryptosystem for IoT devices with limited resources.

- Achieving efficiency and high security for resource-limited devices is a challenging task. To accomplish both of these objectives simultaneously, we use a hyperelliptic curve (HEC), which has exceptional dominance in cryptosystems due to its small key size and high security.
- The proposed algorithm is based on hyperelliptic curve parameters. HEC computational operations are significantly faster than EC operations. This method attains reduced computational cost and increased efficiency, while its smaller key size reduces communication overload.
- We complete a performance evaluation in terms of computational cost and bandwidth overload in comparison to existing techniques and to verify the efficiency of the proposed algorithm. The evaluation results provide evidence that the proposed solution is appropriate and well-suited for resource-constrained environment.
- We validate and verify essential security properties using formal and informal methodologies, ensuring essential security attributes and the achieving of the desired security of the proposed algorithm required for the IoT framework.

The rest of the manuscript is organized into the following sections. *Related Work:* This section describes recent efforts and work that provide the basis of our study. *Proposed Methodology:* This section outlines the design of an efficient and provable cryptosystem for Internet of Things devices based on hyperelliptic curve cryptography suitable for resource-limited devices. We provide a comprehensive analysis and proof of the designed algorithm along with the essential security properties of the proposed cryptosystem. *Results Analysis:* We perform an efficiency comparison of the proposed algorithm with existing schemes in terms of communication and computational cost; we also provide a formal analysis for validation and verification of the proposed cryptosystem.

3. Related Work

With IoT-based architectures, two primary concerns are authenticity and data security due to the open nature of the Internet. Digital signatures are implemented to ensure the integrity [23], while encryption is used to secure the data during digital communication [24]. However, the resource-intensive architecture of the Internet of Things makes it difficult to execute both of these processes independently. In I997, Zheng developed an algorithm that performs the functionalities of both encryption and signatures together in a single process and termed it as signcryption [25]. The revolutionary algorithm saves up to 50% computational cost and 85% bandwidth cost in comparison to previously proposed sign-then-encrypt or encrypt-then-sign techniques [26]. The working of the algorithm is based on the idea of a public-key cryptosystem (PKC) [27]. Conventional public key infrastructure (PKI) relies on a trusted third party, the certificate authority (CA), which is responsible for managing and distributing users' public keys and certificates. PKI has gained acceptance in IoT e-commerce applications as it requires a reliable certificate authority (CA) to issue certificates for public keys and the corresponding identity of the key holder, thus ensuring the validity of this relationship through the CA's digital signature [28]. PKI-based cryptosystems are not suitable for resource-limited IoT devices as they lead to high storage and computational costs required for the management and storage of certificates, and also, they need extra computational time to verify public keys before use [29]. To reduce these difficulties, identity-based cryptosystems (IBCs) have been introduced. In an identity-based system, individuals are allowed to generate a public key based on their known identity, which can be a string. A third party, known as the private key generator (PKG), is responsible for generating the corresponding private key. The PKG publishes the master public key while retaining the master private key [30]. In an identity-based cryptography (IBC) system, the trusted private key generator (PKG) generates the corresponding private key using the system's master secret key, which eliminates the need for users to verify the validity of public keys (which are meaningful strings) and store user certificates [31].

Generally, security schemes are evaluated on the basis of computationally hard problems like Revest–Shamir–Edelman (RSA), bilinear pairings (BPs), Diffie–Hellman (DH), and elliptic curve cryptography (ECC) [32]. The RSA cryptosystem uses 1024-bit keys due to its significant map-to-point computation and operational features. A BP is considered approximately 14.31% less efficient than RSA [33]. ECC was created to overcome the drawbacks of RSA and BP by reducing the key sizes; it requires 160-bit short keys for security efficiency and hardness [34]. These comparisons demonstrate how ECC outperforms in comparison to other cryptographic techniques in terms of both security and performance [35]. A novel type of cryptosystem called hyperelliptic curve cryptography (HECC) is introduced, which can be an extension or generalized of ECC. HECC offers a security level comparable to that of BP, RSA, DH, and ECC but with shorter key lengths: approximately 80 bits in size [36].

The key objective of cryptographic protocols is to provide security while ensuring the confidentiality and authenticity of data. Due to the distributed and resource-limited nature of IoT architecture, various types of cryptosystems have been implemented according to specific usage and computing requirements [37]. PKC and IBC are considered more appropriate solutions that are used for providing secure communications for IoT frameworks [38]. Several researchers have provided diverse techniques and solutions, each based on their research. By integrating several methodologies, these suggestions provide considerable advantages for the design and implementation of secure and efficient cryptosystems for IoT frameworks. Authors have presented a signcryption scheme based on elliptic curve cryptography that combines ECDSA and PSCE-1 and offers public verifiability and resistance against adaptively chosen cipher-text attacks. It achieves communication cost savings of at least 1.25 times, improves computation times compared to ECDSA-then-PSCE-1, and utilizes a uniform elliptic curve cryptosystem platform, eliminating the need for multiple cryptosystem components. The scheme is secure and efficient and can be implemented in software and hardware at a low price. Additionally, the article introduces a broadcast scheme for multiple recipients and a threshold scheme with distributed key generation

for multiple senders [39]. Libert, B., et al. proposed a new identity-based signcryption approach that uses pairings over elliptic curves. The system combines signature and encryption features and has been shown to be secure in the random oracle model. The suggested approach is compared to existing methods in terms of security and efficiency, and a proof of semantic security is provided using the decisional bilinear Diffie–Hellman assumption; the scheme proves advantageous in terms of security and efficiency [40]. Significant security concerns in IoT applications have been identified by researchers [41]. Several cryptographic solutions have been developed to address these challenges maintaining the privacy and security of data transmitted by resource-constrained devices [42,43]. Various signcryption approaches have been employed to tackle security concerns within the IoT architecture framework which are concentrated on the key issues associated with different cryptographic algorithms. Considering major cryptographic features such as security strength, power consumption, and memory optimization [44]. To address limitations of resources in IoT technologies, lightweight cryptographic (LWC) approaches have been suggested [45]. The authors present a certificateless hybrid signcryption system based on bilinear computation, which they recognized to be computationally lightweight and secure in terms of computational utilization [46]. The authors pointed out the drawbacks of previous techniques and proposed a hybrid signcryption scheme for the IoT to overcome these challenges [47]. To reduce computing costs and transmission overhead, some authors have suggested an EPFIBSC method based on elliptic curve cryptography; they compared its performance and security accomplishments to those of other proposed schemes [48]. Zhang et al. developed the CGSC scheme, which was designed specifically for resource-constrained devices; it provides an efficient solution without requiring bilinear operations and overcomes the limitations of existing techniques [49]. Zhou et al. developed the CP-EHSC IoT approach for heterogeneous systems based on elliptic curve cryptography, performed a cryptanalysis, and claimed it had higher security and efficiency achievement in comparison to existing solutions [50]. However, the methodology they used required large computational costs and communication overhead, and it also lacks primary security essentials required for secure transmission of data in the IoT architecture framework. The aforementioned comparative research shows that the majority of existing methods are not suitable for the IoT framework due to their high computational and bandwidth requirements also lacks of essential security features makes these cryptographic vulnerable to several threats. Considering the security and efficiency requirements in a heterogeneous IoT environment, we have proposed a novel signcryption method designed for resource-constrained IoT environments. Our technique optimizes efficiency and provides protection against numerous attacks.

3.1. Preliminaries of Elliptic Curve Cryptography

An elliptic curve is an algebraic curve as shown in Figure 2, and it can be mathematically expressed by Equation [51]:

$$C : y^2 = x^3 + ax + b \tag{1}$$

In Equation (1), parameters a and b are constants that define the shape and characteristic of the curve, and x and y are variables that represents the coordinates of the curve that satisfy the equation. Suppose F_p C to be a prime function field defined over curve C and that can be expressed as C $(F_p)\{(x, y) \in F(p)$, where $p = (x, y) \cup (\infty)\}$, where ∞ being the point at infinity on the elliptic curve [52].

Elliptic curve (EC) theory is the most recent and advanced technique used for modern cryptography: known as elliptic curve cryptography (ECC). ECC is commonly used to enhance the security of open communication networks and significantly improves security and efficiency. ECC is an improved version of public-key cryptography (PKC) that offers more security than other types of data encryption techniques currently used [53]. ECs' mathematical structure and algebraic operations make these curves most suitable for use in cryptography. ECC can be used to encrypt and decode data [54], generate and exchange keys, and to create digital signatures [55,56].

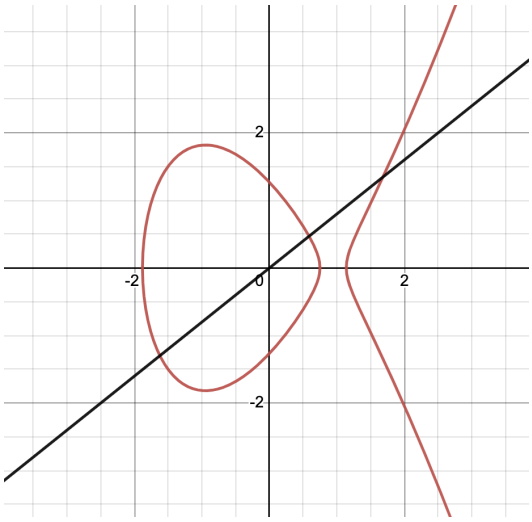

Figure 2. Elliptic curve.

3.2. Hyperelliptic Curve

A hyperelliptic curve (HEC) is the generalized form of an elliptical curve (EC), as illustrated in Figure 3. According to [57], hyperelliptic curve C of genus G is an imaginary quadratic model and can be mathematically expressed:

$$C : y^2 = f(x) \; where \; f(x) \in F_p(x) \; and \; \deg f = 2y + 1 \tag{2}$$

Suppose F_p C is a function field defined over C and that can be expressed as $C(F_p) = \{(u, v \in F_p.(V^2) \; = f_u \; \cup (\infty)\}$, where ∞ is the point at infinity on the hyperelliptic curve.

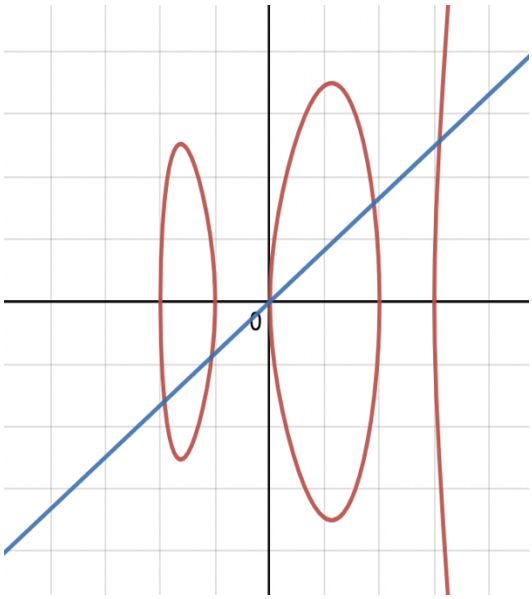

Figure 3. Hyperelliptic curve.

The hyperelliptic curve is a type of algebraic curve that is considered to be a generalized variant of the elliptic curve. An EC is a curve with a genus (G) value of 1, while an HEC has a genus value greater than 1. Curves with a genus value of 1 in the finite field F require 160-bit-long operands Θ for group order (g). Hence, mathematical operations within the finite field require at least $g \log 2^{(\Theta)} = 2^{160}$, while curves with a genus value of 2 or greater require only 80-bit-long operands. The characteristic of HEC with respect to RSA, EC, and bilinear pairing is that HEC provides the same security level with a smaller parameter size [58].

3.3. Elliptic Curve Discrete Logarithm Problem (HECDLP)

The security of ECC relies on the existence of a trapdoor or one-way function, enabling efficient calculations in one direction while rendering it computationally impractical to determine the solution in the opposite direction. This involves determining the solution for random elliptic curve elements corresponding to publicly known base points. The challenge of solving this problem is referred to as the elliptic curve discrete logarithm problem (ECDLP) [59].

Suppose there is a divisor D having order of q which belongs from the *Jacobian Group* (F_q) mathematically equation can be expressed as: $D_1 = L_1 \cdot D$ where $L_1 \in F_q$ therefore finding integer L_1 is called hyperelleptic Curve Discrete Logrithm problem [60].

HECC is an extension of elliptic curve cryptography (ECC) that operates on hyperelliptic curves, which are defined by Equation (2) to have the form $C : y^2 = f(x)$, where $f(x)$ is a polynomial of higher degree compared to the cubic equation used in ECC. Like in ECC, the discrete logarithm problem (DLP) plays a fundamental role in the security of hyperelliptic curve cryptography (HECC).

HECC gains dominance in cryptosystems due to its minor key size, low computational cost, bandwidth savings, high speed, and decreased power consumption. Furthermore, its light weight makes it salutary for wireless sensor networks, web servers, e-commerce, IoT, and cryptocurrency. All these competencies make it possible to implement it in hardware as well as in software. Considering these advantages, HECC is a convenient choice for IoT devices to achieve efficiency and high security with fewer resources and limited computation.

4. Proposed Methodology

This section covers the system initialization phase for the proposed methodology.

4.1. System Setup Phase

The proposed cryptosystem is PKI-based, and the functionality of the algorithm is based on a key generation center (KGC). The algorithm's characteristics depend on the initialization of the system in a few steps. The KGC maintains the list of public attributes. The proposed scheme comprises the following three phases: key generation phase (Section 4.2), signcryption phase (Section 4.3), and unsigncryption phase (Section 4.4). Table 1 depicts the basic notations used in the proposed algorithm. Similarly, Figure 4 highlights the importance of the notations used in the proposed algorithm and provides sufficient reasoning for each part of the proposed system. It also demonstrates how these parameters are utilized in each step of the proposed methodology.

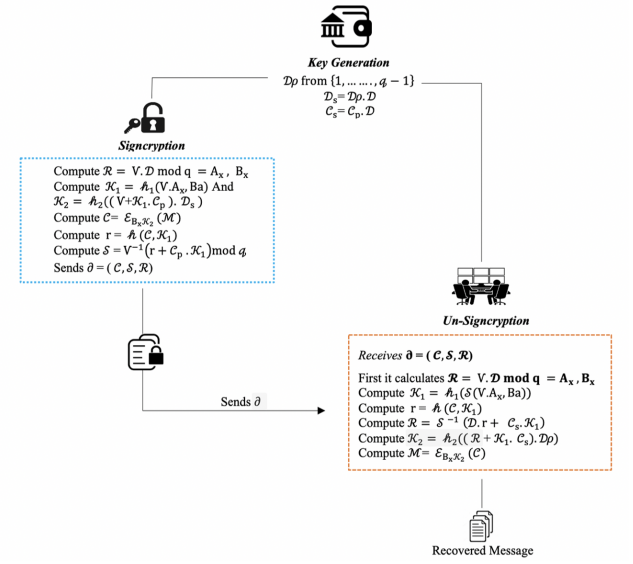

Figure 4. Proposed algorithm working overview.

Table 1. Basic notations for proposed algorithm.

D	Divisor on Generalized Hyperelliptic Curve
C_p	Private Key of IoT Node
C_s	Public Key of IoT Node
D_s	Control Center Public Key
D_p	Control Center Private Key
$\hbar, \hbar_1, \hbar_2$	Hash Functions
C	Cipher Text
B_a	Fresh Nonce
M'	Encrypted Message
K_1,K_2	Secret Keys

4.2. Key Generation

The private-key generator (PKG) generates the private key D_p from $\{1, \ldots, q-1\}$, where $q = 2^{80}$, and public key $D_s = D_p \cdot D$. Likewise, private keys can be calculated as $C_s = C_p \cdot D$ using HEC for the IoT devices in the proposed system architecture. On the basis of the chosen private keys, public keys are derived from a point on the hyperelliptic curve, e.g., $D_s = D_p \cdot D$; this is known as the HECDLP.

4.3. Theorem—IoT Device Signcryption

Select a random number $v \in \{1, \ldots, q-1\}$ and a fresh nonce B_a before sending tuple $\{C,S,R\}$ to the control center.

i. And then, compute $R = v \cdot D \bmod q$, $A_x \cdot B_x$;
ii. Compute $K_1 = \hbar_1 (v \cdot A_x, B_a)$ and $K_2 = \hbar_2 (v + (K_1 \cdot C_p) \cdot Ds)$;
iii. Compute $C = E_{B_x} K_2 (M')$;
iv. Calculate $\gamma = \hbar (C, K_1)$;
v. Calculate $S = v^{-1} (\gamma + C_p \cdot K_1) \bmod q$;
vi. Send $\delta = \{C,S,R\}$ to the control center.

4.4. Theorem—Control Center Unsigncryption

Upon recieving the alert message or encrypted data frames from the IoT nodes $\delta = \{C,S,R\}$, the control center will performs the following steps to decrypt the signcrypted message Firstly, the control center computes $R = v \cdot D \bmod q, = A_x, B_x$

i. Compute $K_1 = \hbar_1 (S(v \cdot A_x \cdot B_a))$;
ii. Compute $\gamma = \hbar (C, K_1)$;
iii. Compute $R = S^{-1} (D \cdot \gamma + C_s \cdot K_1)$;
iv. Compute $K_2 = \hbar_2 ((R + K_1 \cdot C_s) \cdot D_p)$;
v. Compute $M' = E_{B_x} K_2 (C)$.

Receive tuple $\delta = \{C,S,R\}$; then, decrypt it to recover the actual data.

4.5. Correctness Proof of Algorithm

Proof. The following calculations were performed by unsigncrypter to create a secret session key:
$K_2 = \hbar_2 (R + K_1 \cdot C_s \cdot D_p)$ and it should be equal to
$\hbar_2 (v + K_1 \cdot C_p \cdot D_s)$
$= \hbar_2 ((v \cdot D + K_1 \cdot C_s) \cdot D_p)$ where $R = v \cdot D$
$= \hbar_2 ((v \cdot D + K_1 \cdot C_p \cdot D) \cdot D_p)$ where $C_s = C_p \cdot D$
$= \hbar_2 ((v + K_1 C_p) D \cdot D_p)$ where $D_s = D \cdot D_p$
$= \hbar_2 (v + K_1 \cdot C_p) \cdot D_s) = K_2$ □

Proof. If any conflict occurs between the signcrypter and the unsigncrypter, the following calculations are perform by the trusted third party (TTP) to resolve the conflict easily by using the formula:

$R = K^{-1}\ (D{\cdot}\gamma + C_s{\cdot}K_1)$

In the above formula, K^{-1} can be calculated as $\frac{(D \cdot \gamma + C_s K_1)}{S}$; hence,

$\Rightarrow R = \frac{(D{\cdot}\gamma + C_s K_1)}{S}$ where $S = v^{-1}(\gamma + C_p \cdot K_1)$

$\Rightarrow \frac{(D{\cdot}\gamma + C_s K_1)}{v^{-1}(\gamma + C_p{\cdot}K_1)}$

$\Rightarrow \frac{(D{\cdot}\gamma + C_p{\cdot}D{\cdot}K_1)}{v^{-1}(\gamma + C_p{\cdot}K_1)}$ where $Cs = Cp.D$

$\Rightarrow R = \frac{D(\gamma + C_p{\cdot}K_1)}{v^{-1}(\gamma + C_p{\cdot}K_1)}$

$\Rightarrow \frac{D}{v^{-1}}$ where $Dv = R$ $\square$

5. Security Analysis and Correctness Proof

This section highlights the comprehensive analysis of the essential security attributes and their mathematical proofs as offered by the proposed algorithm. These attributes are the founding pillars of security as they essentially play a pivotal role in secure communication:

5.1. Confidentiality

Transmitted data confidentiality can be accomplished with the assistance of Equations (3) and (5) in Sections 5.2 and 5.3 for signcryption and unsigncryption processes, accordingly.

5.2. Signcryption Process

K_2 in Equation (3) provides confidentiality during the signcryption process. In order to temper the confidentiality during the signcryption process, it is compulsory to obtain C_p from Equation (4). Subsequently, it becomes crucial to find the solution of Equation (5) which is unsolvable due to its reliance on HECDLP.

$$K_2 = \hbar_2(v + K_1 \cdot C_p) \cdot D_s \tag{3}$$

$$C_s = C_p \cdot D \tag{4}$$

$$R = v \cdot D \tag{5}$$

5.3. Unsigncryption Process

Equation (6) shows that K_2 ensures confidentiality during the unsigncryption process. In order to temper the confidentiality during the unsigncryption process, it is compulsory to obtain D_p from Equation (7); then, it is vital to solve Equation (5). It is practically not possible to generate the original data from a solution of HECDLP two times.

$$K_2 = \hbar_2(R + K_1 \cdot C_s \cdot D_p) \tag{6}$$

$$D_s = D \cdot D_p \tag{7}$$

Hence, in the proposed architecture framework confidentiality of data is proven at both ends IoT node (signcrypter end) and the control center (unsigncrypter end).

5.4. Integrity

During encryption of C, Equation (8) depicts that the sensing unit of the IoT must first validate (v) by means of bypassing the hash function ($\hbar$) with the assistance of (K_1). The control center first checks the freshness of B_a after obtaining data from IoT nodes; then, it will calculate its hash value from Equation (9). If the attacker succeeded at modifying the encrypted data, then changes from C to C' are spotted by the devices due to the collision-resistance property of hash functions $\hbar$ and $\hbar_2$.

$$\gamma = \hbar(C \cdot K_1) \tag{8}$$

$$K_1 = \hbar_1(S(v \cdot A_x \cdot B_a)) \tag{9}$$

5.5. Authenticity

In the proposed architecture framework, data authenticity for the data captured by IoT sensor nodes can be achieved by performing the following calculations. The control center extracts A_x, B_x by calculating $\hbar_2(R + K_1 \cdot C_s) \cdot D_p = \hbar_2(v + K_1 \cdot C_p) \cdot D_s = K_2$. Moreover, the control center checks the validity of A_x, B_x after decrypting cipher text (C).

5.6. Replay Attack Resistance

Our scheme ensures resistance against replay attacks. If an attacker wants to resend an old data set, then it is required to generate the tuple $(\delta) = (C,S,R)$ and send it to the control center. Upon receiving (δ), the control center first checks the B_a freshness: if B_a has a fresh value, then tuple $(\delta) = (C,S,R)$ is accepted; otherwise, it is rejected.

5.7. Unforgeability

In order to produce a forged signature, the forgery requires Equation (9). But the forger will need to find the value of the private random number v and the sender's private key C_p to solve Equations (4) and (5). As mentioned above in Section 5.2, it is not feasible to solve HECDLP. Hence, the proposed work satisfies protection against unforgeability.

$$S = v^{-1}(\gamma + C_p \cdot K_1) \tag{10}$$

5.8. Forward Secrecy

As for the assumption if unluckily the private key C_p of any IoT node is compromised the attacker will still unable to decrypt the original message and data contents because in this situation the intruder must need to penetrate into the direction of secret key to access data. Therefore, to generate the secret key K_2 as illustrates by Equation (3) in Section 5.2 the attacker needs random number v which is private and only known to the signcrypter. On the other side, if the unsigncrypter's private key D_p is compromised the infiltrator needs to calculate K_2 from Equation (4) to attain R; this still remains infeasible for the adversary to solve the equation due to HECDLP hardness. Furthermore, Equations (3) and (4) are associated with random number v and K_1 is the commitment to unsolvability of the equations and also ensures the guarantee of forward secrecy for the proposed algorithm.

5.9. Public Verifiability

With regard to public verifiability, the third person Trusted Certificate Authority (TCA) endorses that the signcrypted message is valid and verifies the integrity and confidentiality of the scheme. The TCA verifies it without knowing the private keys (neither the recipient's key nor the sender's key) of any party. TCA ensures and verifies absence of tampering in the original data.

5.10. Non-Repudiation

Our scheme achieves non-repudiation through the utilization of Equation (10), which verifies that IoT nodes cannot deny their ownership of the data or their actions taken on the data forwarded to the control center. Moreover, this property can be easily justified using the second Proof illustrated in Section 4.5.

5.11. Protection Lifetime

The assurance of non-renouncement and privacy remains in effect throughout the entire lifespan of the information, starting from its creation at the IoT node. These measures ensure the protection of all information before it is transmitted from the IoT node. Consequently, there is no need to doubt the trustworthiness of the cloud service provider in terms of maintaining data privacy and reliability.

5.12. Denial of Service

The key generation center cannot access either plain text nor encrypted text. Moreover, in place of an authentic IoT node no false message can be sent by any forged node to overburden the control center in the proposed system. In such a manner, the designed cryptosystem preserves security and imparts resistance against denial-of-service attacks.

6. Results

6.1. Security Analysis

The purpose of this section is to evaluate the security requirements for the proposed algorithm. The security requirements, which are indicated in Table 2, can be considered to be the baseline security needs for any secure system. Therefore, it is essential to consider these needs while developing secure cryptosystems. In Section 5, we highlight the security attributes guaranteed by the proposed algorithm and provide their correctness with strong mathematical proofs. Table 2 depicts a security attribute comparison of the proposed algorithm with the methods of refs. [49,50], where ✓shows the presence of a particular security property offered by the each algorithm.

Table 2. Security Attribute comparison of proposed algorithm with refs. [49,50].

Security Property	Ref. [49]	Ref. [50]	Proposed
Confidentiality	✓	✓	✓
Integrity	✓	✓	✓
Authenticity	×	✓	✓
Replay Attack Resistance	×	✓	✓
Unforgeability	✓	✓	✓
Forward Secrecy	×	×	✓
Public Verifiability	✓	×	✓
Non-Repudiation	✓	✓	✓
Lifetime Protection	×	×	✓
DoS Protection	×	×	✓

6.2. Computational Complexity Analysis

The main parameter to be used for measuring performance is computational time, and the frequent way used for determining computational cost is calculation of the total time it takes to complete the process. The process consists of several major mathematical operations, including pairing operation P, pairing-based scalar multiplication $PBSM$, bilinear pairing BP, exponential operation E, elliptic curve scalar multiplication or point multiplication $ECPM$, and hyperelliptic divisor multiplication $HECDM$ [60]. Based on experimental results, the execution time (ET) for basic operation $ET_P = 20.04$ m·s, and $ET_{PBSM} = 6.38$ m·s [61]. In accordance with experimental results $ET_{BP} = 5.4$ m·s [62]. Furthermore, based on experimental results, $ET_{ECPM} = 2.21$ m·s and $ET_{HECDM} = 1.105$ m·s [63].

To compare the computational cost of the proposed method in contrast to those of existing schemes, we make the following assumptions based on elliptic curve point multiplication $ECPM$ and hyperelliptic curve divisor multiplication $HECDM$ operations. The computational time complexity can be calculated by adding up the number of operands required to complete each step. This measure estimates the time required to execute a computing activity based on the number of operations and the complexity of each operation involved. By examining the amount of operands and their time dependencies throughout the algorithm, we can evaluate the computation's efficiency.

Table 3 depicts the computational cost calculations and a comparison of the proposed algorithm with refs. [49,50] in terms of cost and time complexity with respect to curve operands. The algorithms proposed in refs. [49,50] are based on an elliptic curve point multiplication (ECPM) operation, which requires more execution time and leads to high computational cost [61]. The time complexity of ref. [49] can be calculated by adding the

number of operands involved in each step: it required four *PM* operations for signcryption at the sender's side and five *PM* operations for unsigncryption at receiver's side—hence, nine *ECPM* operations altogether. Likewise, the methodology introduced by ref. [50] utilized two *ECPM* operations for signcryption and five *ECPM* operations for unsigncryption—a cumulative of seven *ECPM* operations. However, our algorithm is based on *HECDM*, which is comparatively faster than *ECPM* [61]: our proposed algorithm implies four *HECDM* operations the at the signcrypter's end and four *HECDM* operations at the unsigncrypter's end—thus, eight *HECDM* operations are required for the entire signcryption process. These results show that the proposed methodology reduces the operational complexity, which increases its computational efficiency. The computational time can be calculated by the time consumed in each step involved. The complexity of the approach presented in ref. [49] was calculated as four *ECPM* operations at the sender's end and five *ECPM* operations at the receiver's end. As a result, the overall computing cost accumulated by this approach is estimated to be nine *ECPM* operations. Single elliptic curve point multiplication *PM* takes about 2.2 m·s, while the hyperelliptic curve divisor multiplication *DM* requires 1.1 m·s [64]. Based on these calculations, the signcryption process is expected to take approximately $ET_{SIGNCRYPTION}$ = 8.8 m·s, while the unsigncryption process is estimated to require $ET_{UNSIGNCRYPTION}$ = 11 m·s. Consequently, the total time calculated for both processes is approximately ET_{TOTAL} = 19.8 m·s [49]. Similarly, $ET_{SIGNCRYPTION}$ = 4.4. m·s, $ET_{UNSIGNCRYPTION}$ = 11 m·s, and ET_{TOTAL} = 15.4 m·s for ref. [50], whereas our proposed methodology requires $ET_{SIGNCRYPTION}$ = 4.4 m·s, $ET_{UNSIGNCRYPTION}$ = 4.4 m·s, and ET_{TOTAL} = 8.8 m·s, as depicted in Figure 5. The outcomes clearly show that the suggested technique minimizes the time complexity while improving the overall efficiency. By optimizing the computational processes involved, the suggested technique achieves faster execution times than the alternative methods in refs. [49,50]. This time complexity reduction allows faster operations that enable IoT devices to perform more efficiently. The improved efficiency of the suggested algorithm has practical results, as it enables fast execution and high performance for a wide range of IoT applications.

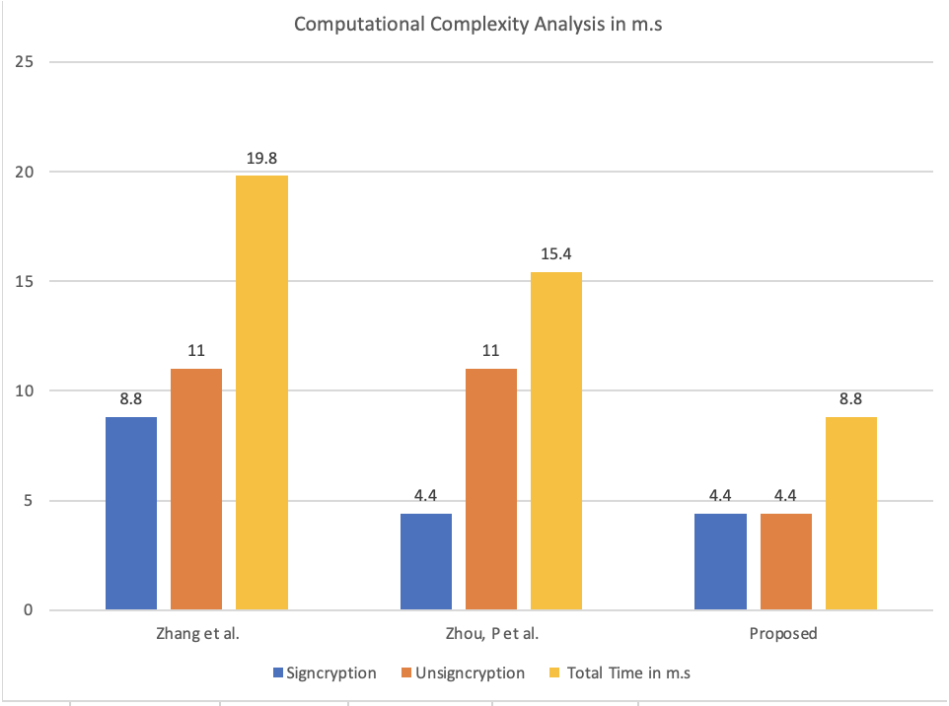

Figure 5. Computational complexity comparison in m·s between ref. [49,50], and the proposed method.

Table 3. Computational complexity analysis.

Scheme	Operands Utilized in Signcryption	Operands Utilized in Unsigncryption	Total Curve Operands Utilized	Time Consumed
Ref. [49]	**4** Elliptic Curve Point Multiplication	**5** Elliptic Curve Point Multiplication	**9** Elliptic Curve Point Multiplication	19.8 m·s
Ref. [50]	**2** Elliptic Curve Point Multiplication	**5** Elliptic Curve Point Multiplication	**7** Elliptic Curve Point Multiplication	15.4 m·s
Proposed	**4** Hyperelliptic Curve Divisor Multiplication	**4** Hyperelliptic Curve Divisor Multiplication	**8** Hyperelliptic Curve Divisor Multiplication	8.8 m·s

6.3. Communication Overhead Complexity Analysis

Communication overhead refers to extra bits added to the actual data and converting it into cipher text. As discussed previously in Section 3.2, ECC requires 160 bits, while HEC provides the same security using 80 bits. Using comparison assumptions for the elliptic curve H and the field size q, with a large prime number $\geq 2^{160}$ as a comparison, the proposed work's parameters are based on an H' hyperelliptic curve, and $u \geq 2^{80}$.

The computational overhead complexity for a cryptographic protocol can be calculated as $|C| + |H| + |q|$, where $|C|$ is the cipher text size used for encryption: as an instance, assume $|C| = 128$ bits. In comparison to the proposed algorithm, the computational overhead of the algorithm proposed in ref. [49] can be calculated as $|C| + |H| + |3q|$, where $|H|$ is 160 bits, and $|3q|$ is $3|160|$ bits. Therefore, the total computational overhead is $|128| + |160| + 3|160| = 768$ bits. Likewise, the computational overhead for the algorithm proposed in ref. [50] can be calculated as $|C| + |H| + 2|q|$, which is $|128| + |320| + |160| = 608$ bits. In comparison, the computational cost of our algorithm is calculated as $|128| + |80| + |80| = 288$ bits. Table 4 reflects a computational overhead comparison at different key sizes $|C|$.

Table 4. Computational overhead complexity analysis.

Scheme	Cipher Size	128 bits	256 bits	512 bits	1024 bits
Ref. [49]	$\|C\| + \|H\| + 3\|q\|$	768	896	1152	1664
Ref. [50]	$\|C\| + 2\|H\| + \|q\|$	608	740	996	1508
Proposed	$\|C\| + \|H'\| + \|u\|$	288	416	672	1184

The efficiency of communication depends on the size of the additional bits. If the additional bits are smaller, the communication will be faster. However, if the additional bits are larger in size, this decreases the efficiency, which causes delays in communication. The comparison results show a significant reduction in communication costs when compared to the previous work in [49,50]. Figure 6 shows the efficient functioning of the proposed methodology at various key sizes. In addition, it also indicates that the proposed solution requires fewer extra bits; thereby, it reduces bandwidth complexity while enhancing overall communication efficiency. This implies that the current proposed work requires fewer computational resources, which makes it a suitable choice for resource-limited IoT devices to perform more efficiently.

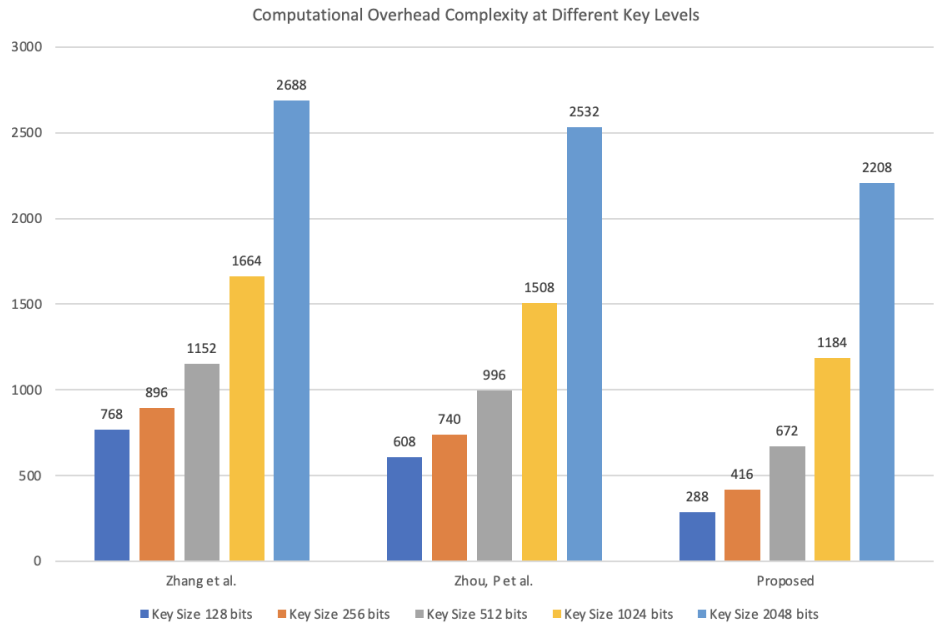

Figure 6. Communication overhead complexity analysis at different key sizes with comparison between [49,50], and proposed method.

6.4. Communication Overhead Reduction

Communication overhead reduction can be calculated with the help of formula [62]:

$$\frac{ExistingScheme - ProposedScheme}{ExistingScheme} * 100$$

We use hyperelliptic curve divisors scalar multiplication, which is faster than previously presented work. We contribute to reduce the computational cost up to 38.16% compared to ref. [49] and 17.6% compared to ref. [50], as depicted in Table 3. The proposed scheme also reduces the communication cost by 62.5% compared to ref. [49] and 52.6% compared to ref. [50], as illustrated in Figure 7.

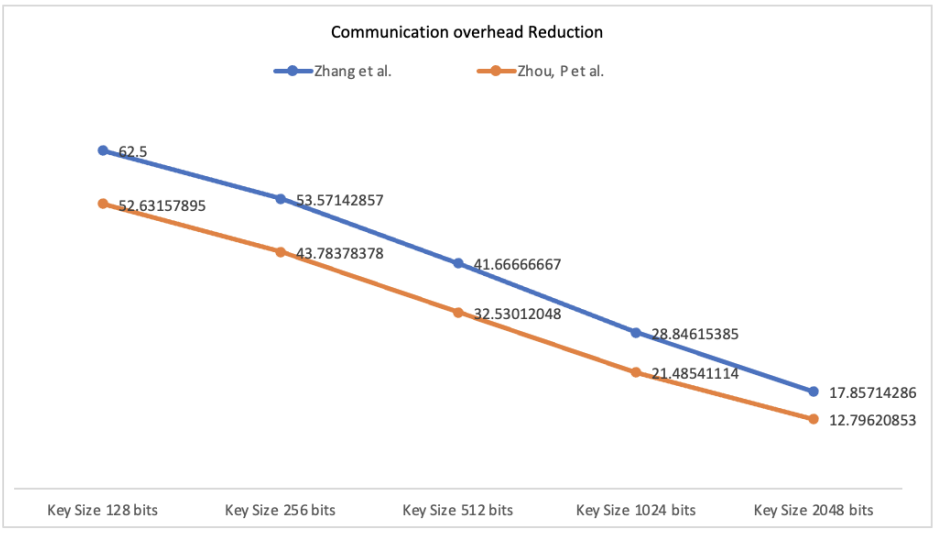

Figure 7. Communication cost reduction comparison of proposed algorithm with [49,50].

6.5. Formal Analysis and Security Validation

This section highlights the formal security verification and validation for the proposed methodology. To validate the security requirements of the proposed scheme, we conducted

an analysis using the AVISPA tool [65,66]. AVISPA employs four back-end protocols—namely, AT-OPMC, AT-AtSe, AT-SATMC, and TA4SP—to verify the functionality of the cryptographic algorithm HLPSL code, which is then converted to IF. The AVISPA tool is seamlessly integrated with SPAN to provide a user-friendly interface. The tool's results are primarily based on two validation states: SAFE and UNSAFE, as shown in Figure 8. If the scheme fails to provide security or resistance against attacks, the validation results summary of the protocol will be labeled as UNSAFE. Simulation results suggest that the proposed protocol has been demonstrated to be secure and suitable for practical implementation. The summary of simulation results for OFMC and ATSE validation as reflected by Figures 9 and 10 further confirm that the algorithm is resistant to cryptographic attacks. Moreover, the instances, roles, and parameters specified in the proposed algorithm are relevant and applicable to real-world scenarios. In conclusion, the evidence presented strongly supports that the proposed protocol is both secure and appropriate for practical use, ensuring that the suggested methodology meets the desired level of security for secure communication in an IoT architecture.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/Proveable/IoT.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 18 nodes
  depth: 6 plies
```

Figure 8. AVISPA results summary.

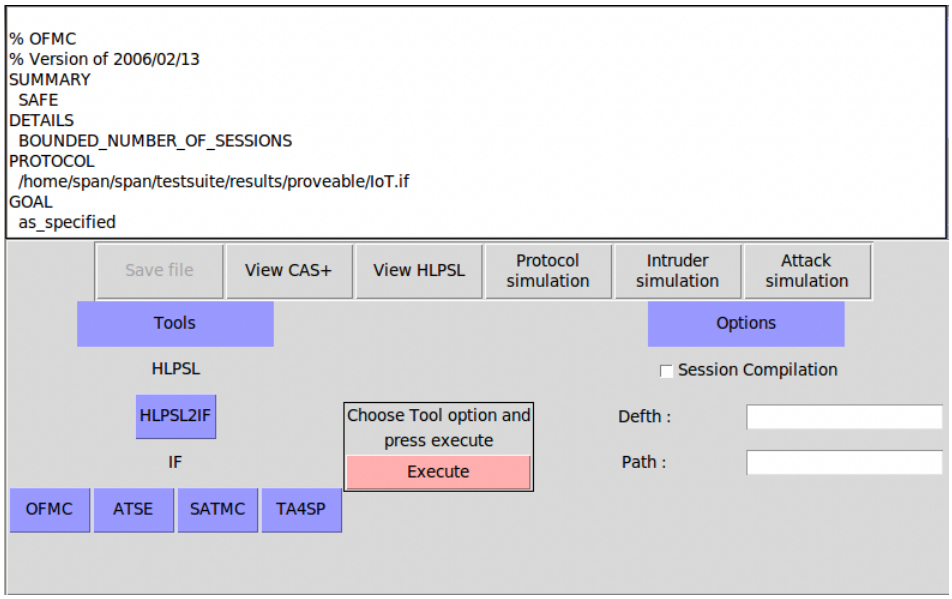

Figure 9. OFMC results summary.

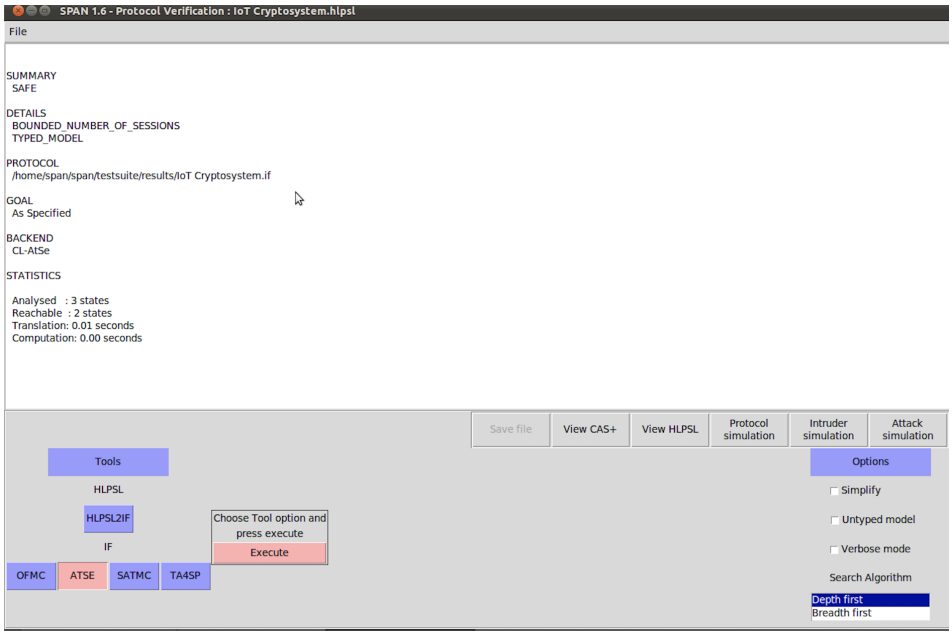

Figure 10. ATSE results summary.

6.6. Discussion

The IoT is the dominant concept in the development of Information Technology and plays an important role by apprehending decidedly sensitive data. The work proposed in this article highlights the security and efficiency challenges in IoT environments. The proposed signcryption algorithm based on hyperelliptic curve cryptography offers a well-balanced solution for resource-constrained IoT devices. It enhances data security by reducing computational and communication complexity and providing high security using a smaller key size. The formal security verification validates its correctness, while comparison results depict the effectiveness of the proposed approach. Overall, the results indicate that the proposed methodology is well-suited for resource-constrained IoT devices by offering improved efficiency and resistance against cryptographic threats. This work contributes to the development of reliable and secure communication channels for IoT devices: ensuring the essential security attributes, i.e., confidentiality, integrity, and authentication of transmitted data. Efficiency is the major requirement for the IoT. Traditional elliptic curve operations, such as point multiplication and point addition, require extensive computations, which may result in negative effects on performance and efficiency. Comparatively, from the analysis presented in Section 6.2, it is evident that our scheme outperforms two previous works: ref. [49] takes 19.8 m·s, and ref. [50] takes 15.4 m·s for the combined signcryption and unsigncryption process, while our proposed scheme only requires 8.8 m·s for the entire process. Additionally, our scheme reduces communication costs by 62.5% compared to ref. [49] and 52.6% compared to ref. [50], as depicted in Figure 7. Furthermore, previous works lack formal analyses or validation proofs for their proposed methods. In contrast, the security of our proposed cryptosystem has been formally investigated using AVISPA. The results analysis is highly satisfactory and clearly demonstrates the superiority of our work over previously presented methodologies. The suggested system holds significant potential for enhancing data security and improving efficiency in IoT devices, and we hope that its practical implementation will help to overcome the security challenges faced by IoT technology.

7. Conclusions

Addressing the security and efficiency concerns inherent in IoT environments is paramount given their resource-constrained and wireless nature. Traditional cryptography methods are often impractical due to their high resource demands. To address these challenges, a novel signcryption algorithm based on hyperelliptic curve divisor multiplication

is introduced. This innovative approach not only offers improved efficiency by being faster and requiring smaller key sizes, but it also enhances security through the use of hyperelliptic curves. By reducing computational and communication complexity, this methodology is well-suited for resource-constrained IoT devices. Furthermore, our methodology includes formal security validation: providing confidence in its practical implementation by reducing the security challenges. The proposed methodology provides a well-balanced solution that meets both security and efficiency requirements to ensure the secure and efficient operation of IoT devices. HECC's characteristics make it an attractive contender for future cryptography applications, especially for IoT devices with limited resources. Continued research, optimization efforts, standardization activities, and improvements in post-quantum cryptography can help HECC become a valuable and widely utilized cryptographic technique in upcoming years, and future research effort can be directed towards advances in optimization methodologies to reduce the computational intensity and make HECC more feasible for resource-constrained devices. This may include efficient implementations and methods designed specifically for HECC that increase performance and reduce the computational complexity.

Author Contributions: Conceptualization, J.K., C.Z., W.A., M.A., and S.A.; Data curation, J.K., W.A., and M.A.; Formal analysis, J.K., W.A., and S.A.; Funding acquisition, M.A. and S.A.; Investigation, M.A. and S.A.; Methodology, J.K., C.Z., W.A., and M.A.; Project administration, C.Z.; Resources, C.Z.; Software, J.K. and W.A.; Supervision, C.Z.; Validation, C.Z., M.A., and S.A.; Visualization, M.A.; Writing—original draft, J.K.; Writing—review and editing, C.Z., W.A., M.A., and S.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to thank Prince Sultan University for paying the APC of this article.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: This research was supported by the EIAS Data Science and Blockchain Lab, Prince Sultan University, Riyadh 11586, Saudi Arabia.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Domínguez-Bolaño, T.; Campos, O.; Barral, V.; Escudero, C.J.; García-Naya, J.A. An overview of IoT architectures, technologies, and existing open-source projects. *Internet Things* **2022**, *20*, 100626. [CrossRef]
2. Azrour, M.; Mabrouki, J.; Guezzaz, A.; Kanwal, A. Internet of things security: Challenges and key issues. *Secur. Commun. Netw.* **2021**, *2021*, 1–11. [CrossRef]
3. Kumari, P.; Jain, A.K. A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Comput. Secur.* **2023**, *127*, 103096. [CrossRef]
4. Ansar, S.A.; Arya, S.; Aggrawal, S.; Saxena, S.; Kushwaha, A.; Pathak, P.C. Security in IoT Layers: Emerging Challenges with Countermeasures. In *Computer Vision and Robotics: Proceedings of CVR 2022*; Springer: Singapore, 2023; pp. 551–563.
5. Al-Shareeda, M.A.; Manickam, S.; Laghari, S.A.; Jaisan, A. Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications. *Sustainability* **2022**, *14*, 15900. [CrossRef]
6. Bout, E. Denial-of-Sleep Attacks on IoT Networks. Doctoral Dissertation, Université de Lille, Lille, France, 2022.
7. Lightbody, D.; Ngo, D.M.; Temko, A.; Murphy, C.C.; Popovici, E. Attacks on IoT: Side-Channel Power Acquisition Framework for Intrusion Detection. *Future Internet* **2023**, *15*, 187. [CrossRef]
8. Alfalouji, Q.; Schranz, T.; Kümpel, A.; Schraven, M.; Storek, T.; Gross, S.; Monti, A.; Müller, D.; Schweiger, G. IoT Middleware Platforms for Smart Energy Systems: An Empirical Expert Survey. *Buildings* **2022**, *12*, 526. [CrossRef]
9. Mali, S.D.; Govinda, K. A study on network routing attacks in IoT. *Mater. Today Proc.* **2023**, *80*, 2997–3002. [CrossRef]
10. Hasan, A.; Khan, M.A.; Shabir, B.; Munir, A.; Malik, A.W.; Anwar, Z.; Ahmad, J. Forensic Analysis of Blackhole Attack in Wireless Sensor Networks/Internet of Things. *Appl. Sci.* **2021**, *12*, 11442. [CrossRef]
11. Kamis, N.H.; Yassin, W.; Abdollah, M.F.; Razak, S.F.A.; Yogarayan, S. Blackhole attacks in internet of things networks: A review. *Indones. J. Electr. Eng. Comput. Sci.* **2023**, *30*, 1080–1090. [CrossRef]

12. Mabodi, K.; Yusefi, M.; Zandiyan, S.; Irankhah, L.; Fotohi, R. Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication . *J. Supercomput.* **2020**, *76*, 7081–7106. [CrossRef]
13. Tatar, E.E.; Dener, M. Wormhole Attacks in IoT Based Networks. In Proceedings of the 2021 6th International Conference on Computer Science and Engineering (UBMK), Ankara, Turkey, 15–17 September 2021. [CrossRef]
14. Gönen, S.; Barışkan, M.A.; Karacayılmaz, G.; Alhan, B.; Yılmaz, E.N.; Artuner, H.; Sindiren, E. A Novel Approach to Prevention of Hello Flood Attack in IoT Using Machine Learning Algorithm. *El-Cezeri* **2022**, *9*, 1529–1541. [CrossRef]
15. Zrelli, A.; Nakkach, C.; Ezzedine, T. Cyber-security for IoT applications based on ANN algorithm. In Proceedings of the 2022 International Symposium on Networks, Computers and Communications (ISNCC), Shenzhen, China, 19–22 July 2022; pp. 1–5. [CrossRef]
16. Kim, M.; Suh, T. Eavesdropping Vulnerability and Countermeasure in Infrared Communication for IoT Devices. *Sensors* **2021**, *21*, 8207. [CrossRef] [PubMed]
17. Sivasankari, N.; Kamalakkannan, S. Detection and prevention of man-in-the-middle attack in iot network using regression modeling. *Adv. Eng. Softw.* **2022**, *169*, 103126. [CrossRef]
18. Chataut, R.; Phoummalayvane, A.; Akl, R. Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0. *Sensors* **2023**, *23*, 7194. [CrossRef] [PubMed]
19. Yildirim, M.; Demiroğlu, U.; Şenol, B. An in-depth exam of iot, iot core components, iot layers, and attack types. *Avrupa Bilim ve Teknoloji Dergisi* **2021**, *28*, 665–669. [CrossRef]
20. Islam, M.R.; Aktheruzzaman, K.M. An analysis of cybersecurity attacks against internet of things and security solutions. *J. Comput. Commun.* **2020**, *8*, 11–25. [CrossRef]
21. Yaacoub, J.P.A.; Noura, H.N.; Salman, O.; Chehab, A. Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet Things Cyber-Phys. Syst.* **2023**, *3*, 280–308. [CrossRef]
22. Taherdoost, H. Security and Internet of Things: Benefits, Challenges, and Future Perspectives. *Electronics* **2023**, *12*, 1901. [CrossRef]
23. Kumar, M.; Verma, H.K.; Sikka, G. A secure lightweight signature based authentication for Cloud-IoT crowdsensing environments. *Trans. Emerg. Telecommun. Technol.* **2019**, *30*, e3292. [CrossRef]
24. Ali, W.; Zhu, C.; Latif, R.; Asim, M.; Tariq, M.U. Image Encryption Scheme Based on Orbital Shift Pixels Shuffling with ILM Chaotic System. *Entropy* **2023**, *25*, 787. [CrossRef]
25. Zheng, Y. Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption). In *Advances in Cryptology—CRYPTO'97, Proceedings of the 17th Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 1997*; Springer: Berlin/Heidelberg, Germany, 1997; pp. 165–179.
26. Singh, A.K. A review of elliptic curve based signcryption schemes. *Int. J. Comput. Appl.* **2014**, *102*, 26–30. [CrossRef]
27. Ye, G.; Jiao, K.; Wu, H.; Pan, C.; Huang, X. An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem. *Int. J. Bifurc. Chaos* **2020**, *30*, 2050233. [CrossRef]
28. Medaglia, C.M.; Serbanati, A. An overview of privacy and security issues in the internet of things. In *The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications*; Springer: New York, NY, USA, 2010; pp. 389–395.
29. Waheed, A.; Iqbal, J.; Din, N.; Islam, S.U.; Umar, A.I.; Amin, N.U. Improved cryptanalysis of provable certificateless generalized signcryption. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*. [CrossRef]
30. Paterson, K.G.; Price, G. A comparison between traditional public key infrastructures and identity-based cryptography. *Inf. Secur. Tech. Rep.* **2003**, *8*, 57–72. [CrossRef]
31. Ting, P.Y.; Tsai, J.L.; Wu, T.S. Signcryption method suitable for low-power IoT devices in a wireless sensor network. *IEEE Syst. J.* **2017**, *12*, 2385–2394. [CrossRef]
32. Challa, S.; Das, A.K.; Gope, P.; Kumar, N.; Wu, F.; Vasilakos, A.V. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems. *Future Gener. Comput. Syst.* **2020**, *108*, 1267–1286. [CrossRef]
33. Khan, M.A.; Ullah, I.; Nisar, S.; Noor, F.; Qureshi, I.M.; Khanzada, F.; Khattak, H.; Aziz, M.A. Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption. *Mob. Inf. Syst.* **2020**, *2020*, 8861947. [CrossRef]
34. Roy, S.; Chatterjee, S.; Das, A.K.; Chattopadhyay, S.; Kumar, N.; Vasilakos, A.V. On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services. *IEEE Access* **2017**, *5*, 25808–25825. [CrossRef]
35. Khan, M.A.; Qureshi, I.M.; Ullah, I.; Khan, S.; Khanzada, F.; Noor, F. An efficient and provably secure certificateless blind signature scheme for flying ad-hoc network based on multi-access edge computing. *Electronics* **2019**, *9*, 30. [CrossRef]
36. ur 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*. [CrossRef]
37. Safi, A. Improving the security of internet of things using encryption algorithms. *Int. J. Comput. Inf. Eng.* **2017**, *11*, 558–561.
38. Zhang, Y.; Deng, R.H.; Zheng, D.; Li, J.; Wu, P.; Cao, J. Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT. *IEEE Trans. Ind. Inform.* **2019**, *15*, 5099–5108. [CrossRef]
39. Han, Y.; Yang, X.; Hu, Y. Signcryption based on elliptic curve and its multi-party schemes. In Proceedings of the 3rd International Conference on Information Security, Shanghai, China, 14–16 November 2004; pp. 216–217. [CrossRef]
40. Libert, B.; Quisquater, J.J. A new identity based signcryption scheme from pairings. In Proceedings of the 2003 IEEE Information Theory Workshop (Cat. No. 03EX674), Paris, France, 31 March–4 April 2003; pp. 155–158. [CrossRef]

41. Tweneboah-Koduah, S.; Skouby, K.E.; Tadayoni, R. Cyber security threats to IoT applications and service domains. *Wirel. Pers. Commun.* **2017**, *95*, 169–185. [CrossRef]
42. Tawalbeh, L.A.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and security: Challenges and solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
43. Nayak, P.; Swapna, G. Security issues in IoT applications using certificateless aggregate signcryption schemes: An overview. *Internet Things* **2022**, *21*, 100641. [CrossRef]
44. Thabit, F.; Can, O.; Aljahdali, A.O.; Al-Gaphari, G.H.; Alkhzaimi, H.A. A Comprehensive Literature Survey of Cryptography Algorithms for Improving the IoT Security. *Internet Things* **2023**, *22*, 100759. [CrossRef]
45. Chiadighikaobi, I.R.; Katuk, N. A scoping study on lightweight cryptography reviews in IoT. *Baghdad Sci. J.* **2021**, *18* (Suppl. 2), 0989. [CrossRef]
46. Gong, B.; Wu, Y.; Wang, Q.; Ren, Y.H.; Guo, C. A secure and lightweight certificateless hybrid signcryption scheme for Internet of Things. *Future Gener. Comput. Syst.* **2022**, *127*, 23–30. [CrossRef]
47. Wu, Y.; Gong, B.; Zhang, Y. An improved efficient certificateless hybrid signcryption scheme for internet of things. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6945004. [CrossRef]
48. Kiran, M.A.; Pasupuleti, S.K.; Eswari, R. Efficient Pairing-Free Identity-Based Signcryption Scheme for Cloud-Assisted IoT. *Int. J. Cloud Appl. Comput. (IJCAC)* **2022**, *12*, 1–15.
49. Zhang, B.; Jia, Z.; Zhao, C. An efficient certificateless generalized signcryption scheme. *Secur. Commun. Netw.* **2018**, *2018*, 3578942. [CrossRef]
50. Zhou, P.; Jin, C.; Chen, Z.; Chen, G.; Wang, L. An efficient heterogeneous signcryption scheme for internet of things. *Pervasive Mob. Comput.* **2023**, *94*, 101821. [CrossRef]
51. Singh, A.K.; Solanki, A.; Nayyar, A.; Qureshi, B. Elliptic curve signcryption-based mutual authentication protocol for smart cards. *Appl. Sci.* **2020**, *10*, 8291. [CrossRef]
52. Eltaieb, R.A.; El-Banby, G.M.; El-Shafai, W.; Abd, El-Samie, F.E.; Abbas, A.M. Efficient implementation of cancelable face recognition based on elliptic curve cryptography. *Opt. Quantum Electron.* **2023**, *55*, 841. [CrossRef]
53. Verma, S.K.; Ojha, D.B. A discussion on elliptic curve cryptography and its applications. *Int. J. Comput. Sci. Issues (IJCSI)* **2012**, *9*, 74.
54. Sajjad, A.; Afzal, M.; Iqbal, M.M.W.; Abbas, H.; Latif, R.; Raza, R.A. Kleptographic attack on elliptic curve based cryptographic protocols. *IEEE Access* **2020**, *8*, 139903–139917. [CrossRef]
55. Ullah, S.; Zheng, J.; Din, N.; Hussain, M.T.; Ullah, F.; Yousaf, M. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Comput. Sci. Rev.* **2023**, *47*, 100530. [CrossRef]
56. Hu, Z.; Lin, D.; Zhao, C.A. Fast scalar multiplication of degenerate divisors for hyperelliptic curve cryptosystems. *Appl. Math. Comput.* **2021**, *404*, 126239. [CrossRef]
57. Pelzl, J.; Wollinger, T.; Guajardo, J.; Paar, C. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. In *Cryptographic Hardware and Embedded Systems-CHES 2003, Proceedings of the 5th International Workshop, Cologne, Germany, 8–10 September 2003*; Springer: Berlin/Heidelberg, Germany, 2003; pp. 351–365.
58. Hosni, A.I.E.; Li, K.; Ahmad, S. DARIM: Dynamic approach for rumor influence minimization in online social networks. In *International Conference on Neural Information Processing*; Springer: Cham, Switzerland, 2019; Volume 12, pp. 619–630.
59. Hosni, A.I.E.; Li, K.; Ding, C.; Ahmed, S. Least cost rumor influence minimization in multiplex social networks. In *International Conference on Neural Information Processing*; Springer: Cham, Switzerland, 2018; Volume 13, pp. 93–105.
60. Debiao, H.; Jianhua, C.; Jin, H. An ID-based proxy signature schemes without bilinear pairings. *Ann. Telecommun.* **2011**, *66*, 657–662. [CrossRef]
61. Hussain, S.; Ullah, S.S.; Ali, I.; Xie, J.; Inukollu, V.N. Certificateless signature schemes in Industrial Internet of Things: A comparative survey. *Comput. Commun.* **2022**, *181*, 116–131. [CrossRef]
62. Fatima, R.; Shaikh, N.S.; Riaz, A.; Ahmad, S.; El-Affendi, M.A.; Alyamani, K.A.Z.; Nabeel, M.; Khan, J.A.; Yasin, A.; Latif, R.M.A. A natural language processing (NLP) evaluation on COVID-19 rumour dataset using deep learning techniques. *Comput. Intell. Neurosci. J.* **2022**, *2022*, 6561622. [CrossRef] [PubMed]
63. Omala, A.A.; Ali, I.; Li, F. Heterogeneous signcryption with keyword search for wireless body area network. *Secur. Priv.* **2018**, *1*, e25. [CrossRef]
64. Ashraf Ch, S.; Nizamuddin, Sher, M. Public verifiable signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem. In *Information Systems, Technology and Management, Proceedings of the 6th International Conference, ICISTM 2012, Grenoble, France, 28–30 March 2012*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 135–142.
65. AVISPA. Automated Validation of Internet Security Protocols and Applications. Available online: http://www.avispaproject.org (accessed on 5 May 2022).
66. Armando, A.; Basin, D.; Boichut, Y.; Chevalier, Y.; Compagna, L.; Cuéllar, J.; Drielsma, P.H.; Héam, P.C.; Kouchnarenko, O.; Mantovani, J.; Mödersheim, S. The AVISPA tool for the automated validation of internet security protocols and applications. In *Computer Aided Verification, Proceedings of the 17th International Conference, CAV 2005, Edinburgh, Scotland, UK, 6–10 July 2005*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 281–285.