


A Survey on Zero-Knowledge Authentication for Internet of Things

Zhigang Chen ^{1,2} , Yuting Jiang ^{3,*}, Xinxia Song ⁴ and Liquan Chen ⁵

¹ College of Digital Technology and Engineering, Ningbo University of Finance and Economics, Ningbo 315175, China

² School of Information and Intelligent Engineering, Zhejiang Wanli University, Ningbo 315100, China

³ State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an 710071, China

⁴ School of Junior, Zhejiang Wanli University, Ningbo 315100, China

⁵ Department of Computer Science, University of Surrey, Surrey GU2 7XH, UK

* Correspondence: jiangyuting@foxmail.com

Abstract: The Internet of Things (IoT) is ubiquitous in our lives. However, the inherent vulnerability of IoT smart devices can lead to the destruction of networks in untrustworthy environments. Therefore, authentication is a necessary tool to ensure the legitimacy of nodes and protect data security. Naturally, the authentication factors always include various sensitive users' information, such as passwords, ID cards, even biological information, etc. How to prevent privacy leakage has always been a problem faced by the IoT. Zero-knowledge authentication is a crucial cryptographic technology that uses authenticates nodes on the networks without revealing identity or any other data entered by users. However, zero-knowledge proof (ZKP) requires more complex data exchange protocols and more data transmission compared to traditional cryptography technologies. To understand how zero-knowledge authentication works in IoT, we produce a survey on zero-knowledge authentication in privacy-preserving IoT in the paper. First, we overview the IoT architecture and privacy, including security challenges and open question in different IoT layers. Next, we overview zero-knowledge authentication and provide a comprehensive analysis of designing zero-knowledge authentication protocols in various IoT networks. We summarize the advantages of ZKP-based authentication in IoT. Finally, it summarizes the potential problems and future directions of ZKP in IoT.

Keywords: zero-knowledge proof; Internet of Things; authentication; security



Citation: Chen, Z.; Jiang, Y.; Song, X.; Chen, L. A Survey on Zero-Knowledge Authentication for Internet of Things. *Electronics* **2023**, *12*, 1145. <https://doi.org/10.3390/electronics12051145>

Academic Editor: Andrei Kelarev

Received: 31 January 2023

Revised: 18 February 2023

Accepted: 22 February 2023

Published: 27 February 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Internet of Things (IoT) is to put human's economic life and social life, production activities and personal activities in an intelligent environment. It realizes the sensing, identification, control of objects, networked interconnection, and intelligent processing of organic unity in a dynamic environment. The great advantage of IoT is that the federations of IoT devices that process data provide unprecedented opportunities to solve unmanageable internet-scale problems. In recent years, with the rapid development of smart devices and high-speed communication networks, the scale of the IoT continues to expand. It offers numerous services in society, industry, and government, by enabling different communication patterns. Meanwhile, IoT devices and systems can suffer from devastating security breaches. The proliferation of smart devices bring potential risks being connecting to the Internet, such as unauthorized node tampering, intelligent awareness of the node's own security, or counterfeit attacks. Therefore, determining the legitimacy of nodes in a complex IoT is necessary but difficult.

As is well-known, authentication is an important method of connecting distrustful nodes. It highly ensures that the connected nodes are legitimate and blocks malicious attempts to successfully access the IoT system in an untrusted environment. Naturally, the authentication factors are always sensitive, such as passwords, personal identification

numbers (PINs), face recognition, fingerprint, etc. The anonymity and privacy of legitimate nodes cannot be protected in traditional authentication protocols. Especially, data and other sensitive information can be intercepted easily by an adversary during the transmission of vulnerable devices for IoT, causing a great threat to users. In the dynamic IoT environment, the need for a lightweight, flexible, and decentralized framework has emerged to address these threats.

Zero-knowledge authentication relies on zero-knowledge proof (ZKP) [1], which is a fundamental notion in cryptography that enables a prover to convince a verifier of the truth of a statement while leaking nothing. It has three core properties:

- *Completeness*: The verifier accepts the prover's statement if it is true;
- *Soundness*: The verifier rejects the prover's statement if it is wrong;
- *Zero-Knowledge*: The verifier grasps nothing from the interaction other than the fact that the statement is true.

To protect the privacy of users, the zero-knowledge authentication protocol attracts more and more attention. The reason is that ZKP has two main advantages over traditional password-based approaches and public key infrastructure (PKI). The first reason is *zero-knowledge*, which enables anonymous communications. It also avoids forgery, man-in-the-middle attacks (MIMA), replay attacks, password attacks, etc. The second reason is *low consumption*, which means less network traffic. Zero-knowledge authentication can reduce the computation complexity and the length of both the proofs by other techniques, such as the Merkle tree. Motivated by the features of ZKP, the main purpose of this survey is to present an overview of zero-knowledge authentication protocols in the IoT domain.

1.1. Contributions

- First, we categorize the privacy challenges according to architectural layers of IoT.
- Next, we discuss the development process and advantages of ZKP in various IoT environments and provide a full analysis of properties of zero-knowledge authentication that have been proposed in the IoT environment.
- Furthermore, we summarize the application of zero-knowledge authentication in different networks of IoT.
- Finally, we summarize the challenges and future research directions for ZKP in IoT.

1.2. Organization

Section 2 provides an overview of IoT, its architectures, and privacy issues. Section 3 discusses the requirements of authentication for IoT. An overview of zero-knowledge proof is provided in Section 4. Section 5 analyzes the advantages of ZKP-based authentication IoT and its application in different networks. Section 6 summarizes the challenges and future research directions. We conclude in Section 7.

2. IoT Architecture and Privacy

2.1. IoT Architecture

IoT architecture is the top-level design of IoT development, which is related to the compatibility, scalability, and interoperability between upstream and downstream products of the IoT industry chain. Similar to the human senses, nerves, and brain, IoT also needs three processes to deal with problems: comprehensive sensing, reliable transmission, and intelligent processing. Therefore, the architecture of the IoT system has three layers [2]: Perception, Network, and Application. The characteristic details description of the related protocols of each layer are presented in Table 1. This architecture provides a general security framework that covers all the components of the IoT and the threats it may face, as shown in Figure 1.

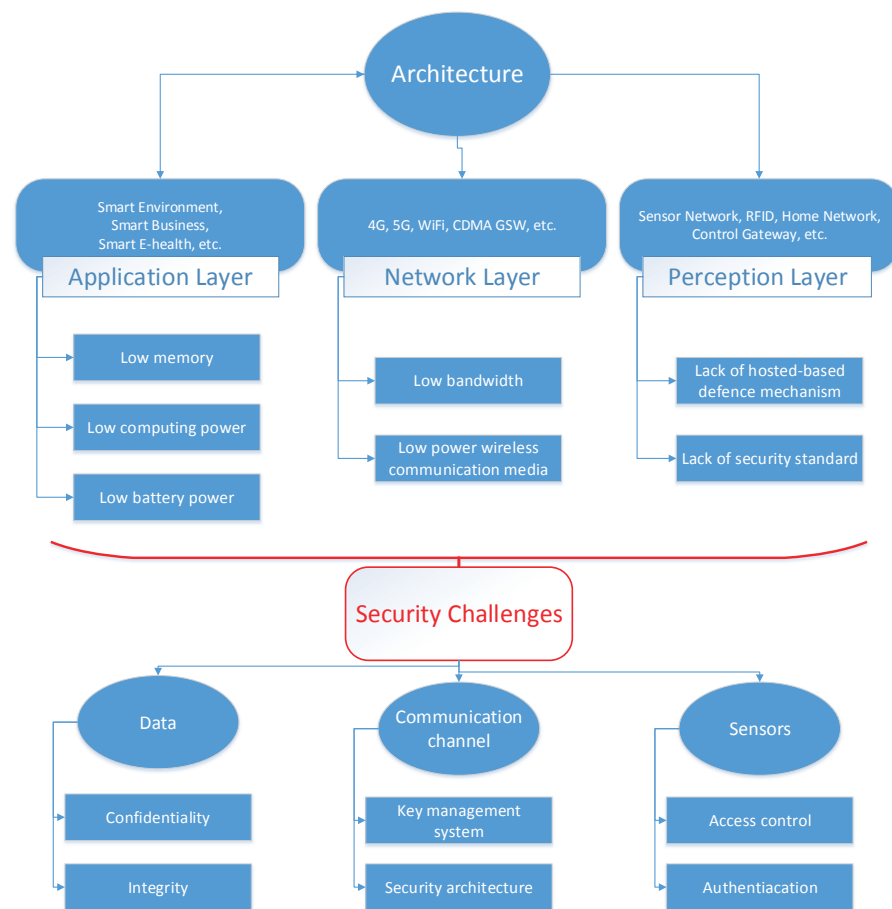


Figure 1. Architecture, bottleneck, and challenge in IoTs.

Table 1. The architecture of the Internet of Things.

Layer	Characteristic	Detailed Description	Related Protocols
Perception	Comprehensive sensing	Utilize RFID, sensors, 1D/2D Code, GPS, and other information sensing devices to obtain information about objects at any time, including user location, individual preferences, physical condition, ambient temperature, humidity, etc.	[3–8]
Network	Reliable transmission	Accurate and real-time delivery of information about objects through various network integrations, service integrations, terminal integrations, and operation management integrations.	[9–14]
Application	Intelligent processing	Utilize various intelligent computing technologies to analyze and process the big data and information obtained from the perception layer, to achieve actual specific application services such as intelligent identification, positioning, tracking, monitoring, etc.	[15–20]

2.2. IoT Security and Privacy

Compared with other web-based information systems, IoT faces more cyber security and privacy threats of information collection, aggregation, transmission, decision making, and controlling. The main reason is the vulnerability of IoT devices and networks since they are resource-constrained.

Macroscopically, in the perception layer, these devices have low computing power and low memory with small battery life; in the network layer, IoT devices deliver information via the low-power wireless communication media and low bandwidth; in the application layer, they lack host-based defense mechanisms and security standardization. These three aspects pose great threats to IoT security, including data security and sensor security in unsafe communication channels.

Microscopically, the design of details of privacy-preserving IoT is a big challenge as well. In IoT, sensitive data can be easily intercepted by adversaries or collected by dishonest devices, such as timestamps, heart rates, daily activities, etc. Exposure to the sensitive data could lead to criminal activity, or even result in serious injury. Unfortunately, the traditional data security and privacy-preserving mechanisms are no longer suitable for resource-constrained devices. Therefore, IoT faces the following challenges: lightweight algorithms, distributed access control, recourse-constrained security architecture, and efficient privacy-persevering mechanisms. In the following, we propose an overview of the privacy concerns and solutions according to the IoT architecture and summarize them in Figure 1.

2.2.1. Network Layer

During data transfer, it is possible to be handed over to one or more networks of different architectures. A common method is to use encrypted data during transmission. Therefore, how to manage the keys and how to design architecture are big issues in IoT.

IoT is the integration of multiple heterogeneous networks, it should deal with compatibility issues between the different networks that are prone to security issues. Key management mechanisms can efficiently solve the problem that establishes the junction of the relation between nodes because legitimate nodes need valid common keys for effective supervision of personal data or corporate secrets. Although a large number of methods have been proposed, the high mobility of users in the IoT, the complexity of affiliation and collaboration, etc., and the difficulty of balancing security levels and resource consumption, in particular, have placed higher demands on key management mechanisms. For distributed sensor networks (DSNs), Eschenauer et al. [9] first proposed a key management scheme to meet its safety and operational needs. Among the nodes of a random graph, they employed a probabilistic key sharing technique to realize shared-key discovery, path-key establishment, key revocation, and so on. Then, Liu et al. [10] proposed a general framework to establish pairwise keys and reduce the computation of sensors' requirements in DSNs. Furthermore, Du et al. [11] proposed a pairwise key predistribution scheme in distributed sensor networks, which greatly improves the networks' resilience. To cause two sensors to share a common key generated using electrocardiogram (EKG) signals, Venkatasubramanian et al. [12] proposed a key agreement scheme in a Body Sensor Network. However, many works that establish key management mechanisms are under trusted third parties, which are not appropriate for an untrusted environment in IoT.

Data networks, especially wireless, are congested during data dissemination due to the large number of devices sending data, resulting in a denial of service provisioning, spoofing, eavesdropping, etc. While some solutions from traditional Internet systems are applicable to the IoT space, the processing and communication capabilities of IoT devices are inherently limited. These capabilities of IoT devices hinder the use of completely developed security suites. Bonetto et al. [13] described a general security architecture along with its basic procedures, then discussed how its elements interact with the constrained communication stack. The general security architecture and its basic procedures are described by Bonetto et al. [13]. The study then discusses how to securely interact with

restricted smart IoT devices. The approach proposed in [13] is lightweight and protects IoT devices with powerful encryption and authentication methods. OSCAR, introduced by Vučinić et al. [14], is an architecture for end-to-end security in the IoT. The architecture authorizes the server to provide users with secret access, enabling them to call for resources from restricted CoAP nodes. Based on the amended secret sharing scheme, Jiang et al. [21] proposed a secure and scalable IoT storage system that supports reliability, flexibility, and scalability at both data and system layers. However, a more stable security architecture is still needed in the face of massive data and complex network environments.

2.2.2. Perception Layer

IoT devices need to collect various data from the physical world, process the data, and store it in the network's database. Therefore, nodes identity authentication and access control to the data are two main techniques to ensure that only legitimate users can use the relevant data, and control the operation of the system.

Within the IoT, many different types of the device will interact. The access control system is a popular technique to check devices' credentials, in which principals and verbs are attached to data items. Then, they decide about devices' access to services and assets. Access control can be divided into two categories: attribute-based encryption (ABE) and identity-based encryption (IBE). ABE encrypts messages based on attributes, without concern for the identity of the recipient, and only users who meet the attribute requirements can decrypt the ciphertext. Based on key-policy ABE, Yu et al. [3] proposed a distributed data access control scheme in wireless sensor networks (WSNs), called FDAC. This scheme enforces fine-grained access control over the sensor data that can resist powerful attacks such as sensor leakage and user colluding. Based on ciphertext-policy ABE, Picazo-Sanchez et al. [4] designed public-subscribe protocols in wireless body area networks (WBANs), to ensure fine-grained and confidentiality access control. Hu et al. [5] proposed an identity-based location system, ensuring that users' location information can be accessed by some authorized users during emergencies. However, the access control systems based on these old cards and cryptographic protocols have several security flaws and can be easily attacked. Ensuring access control is correctly enforced across such networks of heterogeneous devices would be very difficult.

In an untrusted environment, authentication enables the node to use some techniques to prove its legitimacy, including identity authentication and data authentication. Liu et al. [6] designed an authentication protocol for the end nodes in an IoT system, where each node has a unique address in communication. Kalra et al. [7] proposed an ECC-based key establishment technique for IoT that can prevent replay attacks, key control attacks, man-in-the-middle attacks, and eavesdropping. Dwivedi et al. [8] proposed an efficient zero-knowledge-based authentication scheme that authenticates devices on the networks without knowing the information about user identity or revealing any other data entered by users. This approach is mainly suitable for lightweight devices. An efficient zero-knowledge authentication scheme for lightweight devices was proposed by Dwivedi et al. [8]. This scheme allows for authenticating devices without knowing the user's identity or other information. However, the cost of computation and communication in traditional authentication schemes is still high. Therefore, these schemes are not suitable for smart IoT devices due to limitations in memory, energy, and computing power.

2.2.3. Application Layer

Some IoT users submit sensitive data to the collection server, especially in cloud-based IoT. It is very important to anonymize the data before submission so that the collector cannot track it back to the submitter. The bottleneck is that the traditional data protection schemes have difficulty supporting the collection, transmission, and processing of big data, which can cause catastrophic damage to data in the event of an accidental malicious attack. This can be catastrophic to data when an unexpected malicious attack happens. Therefore, it is critical to ensure the integrity, privacy, and security of data. A data masking tool that

simultaneously protects privacy and utility was introduced by Ukil et al. [15]. In IoT data management, the work provides a negotiation-based architecture for the utility–privacy trade-off. Doukas et al. [16] proposed a gateway (GW)-based system that aggregates sensor data. The security issues are solved using PKI data encryption and digital certificates. Furthermore, by storing private data on multiple servers, Yi et al. [17] propose a feasible method to block inside attacks.

A large number of smart devices interactive with each other greatly developing people’s qualities of life and servers to the world economy [22], such as healthcare [23], telecommunication [24], transportation [25], environment control [26], etc. Applications in cognitive radio networks should also be mentioned. Recently, the applications in cognitive radio networks are also gaining attention. Şimşek et al. proposed a fast and lightweight detection and filter approach for low-rate TCP targeted distributed denial of service (LD-DoS) [18]. Savaşçı Şen et al. proposed a surveillance system for the coronavirus pandemic using inter-WBAN geographic routing [19]. Turkyilmaz et al. employed machine learning-based malicious signal detection for cognitive radio networks [20]. From these works, we can see that IoT is closely related to our lives.

These solutions are summarized in Table 2; we can see that IoT needs stronger anonymity, more stable scalability, and lighter algorithms.

Table 2. Solutions to privacy-persevering IoT.

Mechanisms	Scheme	Tools	Features
Key Management	[9]	Probabilistic key sharing	Realizing shared-key discovery, path–key creation, key revocation, etc., in DSNs.
	[10]	Polynomial-based key predistribution protocol	Establishing pairwise keys and reducing the computation at sensors’ requirement in DSNs.
	[11]	Hash-and-MAC	A pairwise key predistribution scheme to improve the resilience of WSNs.
	[12]	EKG	Key agreement scheme with EKG signals.
Security Architecture	[13]	Bootstrapping; Authentication	Lightweight technique with powerful encryption and authentication methods.
	[14]	Digital signature	An architecture for end-to-end security.
	[21]	Shamir’s secret sharing scheme	Supporting reliability, flexibility, and scalability at both data and system layers.
Access Control	[3]	KP-ABE	Enforcing fine-grained access control over sensor data.
	[4]	CP-ABE	Ensuring fine-grained and confidentiality access control.
	[5]	IBE	Ensuring user’s location information is accessed by authorized users.
Authentication	[6]	Code book	Each node has a unique address in communication.
	[7]	ECC	Preventing replay attacks, key control attacks, man-in-the-middle attacks, etc.
	[8]	ZKP	Suitable for lightweight devices.
Confidentiality and Integrity of Data	[15]	Hierarchical-based masking	Appropriate utility–privacy tradeoff in IoT data management.
	[16]	GM	Aggregating sensor data.
	[17]	Paillier Public-Key Cryptosystem	Storing private data on multiple servers.

3. Authentication

Authentication is a pivotal role in determining the legitimacy of a user through user-specific factors on the Internet. For example, the former is the object claiming legitimate access to or use of the latter, and the latter is the system or service for which the claimed legitimacy is determined by authentication. In the following, we introduce the factors and the requirements of authentication.

3.1. Authentication Factors

The accuracy and efficiency of the authentication depend on a number of factors involved in the mechanism. The main factors for authentication of users can be divided into three categories [27]:

- *What you know (knowledge factor)*: Simple to deploy but easy to forget, such as security codes, personal identification numbers (PINs), and passwords.
- *What you have (possession factor)*: Convenient and easy to charge, such as ID cards, random number generators (RNGs), and ATM cards.
- *Who you are (inherence factor)*: Biometric features are divided into physical and behavioral features, physical features include voice, iris, fingerprint, etc.; behavioral features include signature, voice, walking gait, etc.

3.2. Authentication Requirements

Authentication is an important procedure for verifying the identity of an object (human or a machine) [28] to prevent active attacks. The most critical security requirement is to protect users' privacy. However, no generic solution is feasible, as different layers fall under different requirements in the IoT. There are authentication requirements in IoT in the following:

- Lightweight key establishment mechanisms and authentication scheme;
- Frameworks for biometric-based devices;
- Enhanced access control models with dynamics and multiple layers.

3.3. Traditional Public Key Infrastructure Authentication

Public Key Infrastructure (PKI) is the most common authentication technology on the Internet [29,30]. People use the public key certificate method to solve the authentication problem, similar to ID cards, passports, etc. Public key certificates bind entities to a public key and allow other entities to verify the bond. To do this, you need a trusted third party, called a certification authority (CA), to guarantee the entity's identity. The CA is responsible for issuing certificates that contain the entity name, public key, and other identifying information for the body. The Public key infrastructure (PKI) is a secure service facility for hardware, software, personnel, policies, and procedures needed to create, manage, store, distribute, and revoke public key certificates. However, the millions of limited devices that use the IoT currently lack a centralized, scalable system for managing private keys and identities. Centralized management also brings a great threat to privacy security. As a result, the traditional PKI-based authentication model is relatively inefficient in the IoT.

4. Zero-Knowledge Proof

Zero-knowledge proof (ZKP) is a more secure tool with fewer processing resources compared to traditional cryptographic techniques. In the system, the prover has some secrets and the prover manages to prove to the verifier that he has those secrets; the verifier can verify whether the prover really has those secrets, but, at the same time, the verifier does not know those secrets. In this section, we introduce a definition of ZKP, which can be classified as interactive and non-interactive. In interactive zero-knowledge proofs, the prover and verifier exchange many messages. In non-interactive zero-knowledge proofs (NIZK), the prover simply sends a single convincing proof to the verifier. ZKP has

three core properties: completeness, soundness, and zero-knowledge. Therefore, it is an appropriate tool for privacy persevering.

4.1. Interactive Zero-Knowledge Proof

The definition of the interactive zero-knowledge proof system is as follows. Common interactive ZKP includes graph isomorphism and Σ -protocol.

Definition 1 (Interactive ZKP). Let L be a language over $\{0, 1\}^*$ and $(\mathcal{P}, \mathcal{V})$ be an interactive proof system. Let x be of sufficiently large length, $(\mathcal{P}, \mathcal{V})$ is an interactive zero-knowledge proof for L if the following conditions are met:

- **Completeness:** If $\mu \in L$, then $\Pr((\mathcal{P}, \mathcal{V})(\mu)) \geq 1 - \epsilon(|\mu|)$.
- **Soundness:** For any protocol $\hat{\mathcal{P}}$, if $x \notin L$, then $\Pr((\hat{\mathcal{P}}, \mathcal{V})(\mu)) \leq \epsilon(|\mu|)$.
- **Zero-Knowledge:** $|\Pr_{\text{SimV}}(x) - \Pr(\mathcal{P}, \mathcal{V})(\mu)| \leq \epsilon(|\mu|)$,

where $\epsilon(|\mu|)$ is a negligible function.

The Goldreich–Micali–Wigderson (GMW) [31] protocol is an interactive zero-knowledge proof protocol based on a graph isomorphism problem. Let G be an undirected graph consisting of a set of vertices V and a set of edges E between the vertices. There are two graphs $G_0 = (V, E_0)$ and $G_1 = (V, E_1)$ with the same number of vertices. The two graphs are isomorphic, namely, if there is a permutation π on vertices of G_0 ; then, any edge between vertices of G_0 can be mapped to G_1 . See Figure 2 for an example. Given graphs G_0 and G_1 , reorder ABCD to CDAB maps from the first graph to the second. In contrast, there is no known PPT (probabilistic polynomial time) algorithm to determine whether they are isomorphic so far. In the GMW protocol, given two public graphs G_0 and G_1 , the prover convinces the verifier that the graph permutation π is an isomorphism between the graphs. The detailed protocol is seen in Algorithm 1.

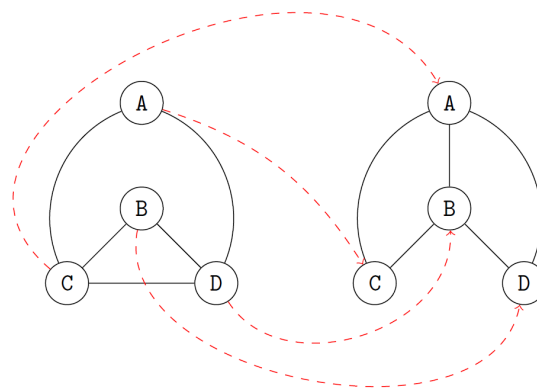


Figure 2. Two isomorphic graphs.

Algorithm 1 Graph Isomorphism-based ZKP.

Require: Two graphs G_0, G_1 with the identical set of vertices V

Ensure: Accept if there is an isomorphism π between G_0 and G_1 ; otherwise, reject.

- 1: The prover set up a random permutation $\rho : V \rightarrow V$ and converts either of the two graphs. They send the resulting initiation graph H to the verifier.
 - 2: The verifier in turn generates a random challenge $b \leftarrow \{0, 1\}$. Then, they ask the prover to provide an isomorphism between G_b and H .
 - 3: The prover can provide correct answer σ to the verifier based on the randomly chosen values b . The detailed answer is seen in Table 3.
 - 4: The verifier accepts the proof if $\sigma(G_b) = H$; otherwise, it rejects.
-

Table 3. The response of prover.

	Answer	Prover's Choice	
		G_0	G_1
Verifier's choice	G_0	ρ	$\rho \circ \pi$
	G_1	$\rho \circ \pi^{-1}$	ρ

To reduce the probability of a malicious prover guessing the verifier's challenge successfully in advance, the Σ -protocol allows the verifier to randomly select the challenge from a larger space as a three-move interactive proof system. The formal definition of Σ -protocol is as follows:

Definition 2 (Σ -protocol). Let R be a polynomial time-decidable binary relation. Let L_R be the language of statements u for which there exists a witness w such that $(u, w) \in R$. For a relation R , a Σ -protocol is a pair $(\mathcal{P}, \mathcal{V})$ of PPT interactive algorithms satisfied

- $m \leftarrow \mathcal{P}(u, w)$: The prover evaluates the initial message m and sends it to the verifier.
- $c \leftarrow S$: The verifier selects a uniformly random challenge c from a large set S and returns to the prover.
- $z \leftarrow \mathcal{P}(c)$: The prover evaluates a response z and sends it to the verifier.
- $1/0 \leftarrow \mathcal{V}(m, c, z)$: The verifier examines the tuple (m, c, z) and returns 1 if he accepts the statement; otherwise, he returns 0.

If the PPT algorithms are complete, sound, and have zero-knowledge, then it is a Σ -protocol.

If the secret that the prover wants to prove is a discrete logarithm (DL), an example of a DL-based Σ -protocol is described in Algorithm 2. The Σ -protocol is following the relation

$$R = \{(u, w) | u = (\mathbb{G}, p, s, t, g, h); s, t, g, h \in \mathbb{G}; s = g^w; t = h^w\},$$

where \mathbb{G} is a group equipped with prime order p , and $g, h \in \mathbb{G}$ are two different generators, and $s, t \in \mathbb{G}$ are two group elements sharing the same discrete logarithm.

Algorithm 2 DL-based Σ -protocol.

Require: $(\mathbb{G}, p, g, h, s, t)$

Ensure: Accept if s, t share the same discrete logarithm or otherwise reject.

- 1: The prover picks a random element r from \mathbb{Z}_p . Then, they compute two blinding elements $a = g^r, b = h^r$, and send them to the verifier.
 - 2: In turn, the verifier selects a uniformly random challenge $c \leftarrow \mathbb{Z}_p$ and returns to the prover.
 - 3: The prover computes the element $z = wc + r$ and sends it to the verifier.
 - 4: The verifier examines whether verification equations $g^z = s^c a, h^z = t^c b$ hold, in which case the verifier accepts the proof; otherwise, they reject it.
-

4.2. Non-Interactive Zero-Knowledge Proof

In practice, the huge communication overhead of the interactive ZKP is not applicable to the IoT, which has a very large number of nodes. To deal with this issue, the idea of non-interactive zero-knowledge proof (NIZK) [32] has emerged in the literature. The formal definition of NIZK is described below:

Definition 3 (NIZK). A non-interactive zero-knowledge proof (NIZK) consists of the three algorithms $(Gen, \mathcal{P}, \mathcal{V})$ described below:

- $crs \leftarrow Gen(1^\lambda)$: On input, a security parameter λ ; output, a common reference string crs .
- $\pi \leftarrow \mathcal{P}(crs, u, w)$: On input, an instance u of some NP-language L_R and the witness w ; output, a zero-knowledge proof π .

- $1/0 \leftarrow \mathcal{V}(crs, u, \pi)$: On input, the proof π ; outputs 1 if accepting; otherwise, 0 if rejecting.

As interacting ZKP, NIZK for relation R is the complete, sound, and zero-knowledge to be defined below.

Definition 4. Let R be a polynomial time-decidable binary relation. Let L_R be the language of statements u for which there exists a witness w such that $(u, w) \in R$. The non-interactive zero knowledge proof system $(Gen, \mathcal{P}, \mathcal{V})$ satisfies the following conditions for all $\lambda \in \mathbb{N}$, all adversaries \mathcal{A} , and all $(u, w) \in R$.

- **Completeness:** $\Pr[\mathcal{V}(crs, u, \pi) = 1 | crs \leftarrow Gen(1^\lambda), \pi \leftarrow \mathcal{P}(crs, u, w)] \approx 1$.
- **Soundness:** $\Pr[u \notin L_R \wedge \mathcal{V}(crs, u, \pi) = 1 | crs \leftarrow Gen(1^\lambda), (u, \pi) \leftarrow \mathcal{A}(crs, u)] \approx 0$.
- **Zero-Knowledge:** if there is a simulator $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ such that

$$\begin{aligned} & \Pr[\mathcal{A}(crs, \pi) = 0 | crs \leftarrow Gen(1^\lambda), (u, w) \leftarrow \mathcal{A}(crs), \pi \leftarrow \mathcal{P}(crs, u, w)] \\ & \approx \Pr[\mathcal{A}(crs, \pi) = 0 | (crs, \tau) \leftarrow \mathcal{S}_1(1^\lambda), (u, w) \leftarrow \mathcal{A}(crs), \pi \leftarrow \mathcal{S}_2(crs, \tau, w)]. \end{aligned}$$

The Fiat–Shamir heuristic is a method for converting public coin interactive zero-knowledge arguments into NIZK proofs.

The Fiat–Shamir heuristic is an efficient way to convert interactive zero-knowledge proofs into non-interactive zero-knowledge proofs. The key idea is that the prover computes the information used in the interactive proof, but replaces the verifier’s information with a hash of the protocol record up to that point. The algorithm is in Algorithm 3.

Algorithm 3 The Fiat–Shamir Heuristic.

Require: (crs, u, w) and a cryptographic hash function H .

Ensure: Accept or reject.

1. The prover runs $\mathcal{P}(crs, u, w)$ and generates the proof π . He hashes the (crs, u, π) to e (e.g., $e = H(crs, u, \pi)$) and sends π and e to the verifier.
 2. The verifier checks if the equation $e = H(crs, u, \pi)$ holds and runs $\mathcal{V}(crs, u, \pi)$ to decide whether to accept.
-

4.3. Summary of ZKP in Recent Years

We summarize the ZKP scheme from different key underlying security techniques in Table 4. It also includes the comparison of communication complexity. Among them, lattice-based ZKP has the ability to resist quantum attacks. In recent years, the research is devoted to solving the problem of the low efficiency of proof generation, and the problem of insufficient universality of underlying assumptions. The series of zero-knowledge proofs that the system parameters can be independently and publicly generated in the start-up stage also appear due to the high credibility requirement in the initialization stage without pretreatment and credibility initialization.

Table 4. Summary of zero-knowledge proof in recent 5 years. Comm. is short for communication. \mathbb{F} denotes the field elements and \mathbb{G} denotes the group elements. C_M represents the number of multiplication gates in the circuit. The data-parallel circuits can be divided into N sub-circuits with width g and depth d . Let λ be a security parameter. β_{SIS} denotes the Module-SIS solution norm. n denotes the required dimension in the lattice problem.

Scheme	Year	Comm. Complexity	Security
GKMMM18 [33]	2018	$3\mathbb{G}$	Bilinear group
Hyrax [34]	2018	$O(d \log Ng)\mathbb{G}$	Sum-check protocol
KKW18 [35]	2018	$O(Ngd)\mathbb{F}$	MPC-in-the-Head
Bulletproofs [36]	2018	$O(\log C_M)\mathbb{G}$	Inner product argument
HKR19 [37]	2019	$O(\log C_M)\mathbb{G}$	Inner product argument
Libra [38]	2019	$O(d \log Ngd)\mathbb{GF}$	Sum-check protocol

Table 4. Cont.

Scheme	Year	Comm. Complexity	Security
Stark [39]	2019	$O(\log Ngd)\mathbb{F}$	Reed Solomon code
Aurora [40]	2019	$O(\log n)\mathbb{F}$	Reed Solomon code
YAZ19 [41]	2019	$\tilde{O}(n^2)$	Lattice
ESLL19 [42]	2019	$\tilde{O}(\lambda \log^2 \beta_{\text{SIS}})$	Lattice
BLS19 [43]	2019	$\tilde{O}(n)$	Lattice
DRZ20 [44]	2020	$O(\log C_M)\mathbb{G}$	Inner product argument
Spartan [45]	2020	$O(\sqrt{n})\mathbb{G}$	Sum-check protocol
Virgo [46]	2020	$O(d \log Ngd)\mathbb{F}$	Sum-check protocol
Ligero++ [47]	2020	$O(\log Ngd)\mathbb{F}$	MPC-in-the-Head
LNS20 [48]	2020	$\tilde{O}(n)$	Lattice
BooLigero [49]	2021	$\frac{O((Ngd)^{1/2})}{(\log \mathbb{F})^{1/2}} \mathbb{F} \sim \frac{O((Ngd)^{1/2})}{(\log \mathbb{F})^{1/4}} \mathbb{F}$	MPC-in-the-Head
Limbo [50]	2021	$O(Ngd)\mathbb{F}$	MPC-in-the-Head
Virgo++ [51]	2021	$\min(O(Ngd), O(d \log Ngd + d^2))\mathbb{F}$	Sum-check protocol
LNP22 [52]	2022	$\tilde{O}(n)$	Lattice

5. Zero-Knowledge Authentication in IoT

Traditional authentication techniques hope to rely on various private factors of the users but not reveal them. However, with the popularization of smart IoT devices, this idea is no longer being realized since smart devices are vulnerable and private data are everywhere. It is easy for attackers to intercept privacy data and steal them. ZKP can be used to prove the truth of someone's statement without leaking any knowledge of the said statement. With the help of ZKP, the identity of the user would be encoded as a hard problem by the prover. Then, the verifier can authenticate the identity using zero-knowledge proof systems. Therefore, ZKP can be used for authentication using anonymous communications. We describe a basic ZKP-based authentication protocol proposed by [53] in Algorithm 4.

Algorithm 4 Zero-knowledge Authentication.

Require: Password and username of the client

Ensure: Accept or Reject

- 1: **Initialization:** Server provides a group \mathbb{G} and randomly chooses a g from \mathbb{G} . Then, set the public key as (\mathbb{G}, g) .
- 2: **Registration:** A user inputs their username and password. The password of the user is hashed by a hash function, i.e., $X = \text{Hash}(\text{password})$. The user computes for $Y = g^X$ and sends it to the server. Then, the username and Y are stored by the server.
- 3: **Authentication:** The server picks random a , stores it, and sends to the user. The user samples a random $r_X \in \mathbb{G}$, and computes $T_1 = g^{r_X}$, $c = \text{Hash}(Y, T_1, a)$ and $z_X = r_X - cX$. Then, he sends (c, z_X) to the server. The server calculates $T_2 = Y^c g^{z_X}$ and checks whether $c = \text{Hash}(Y, T_2, a)$ holds or not. If the equality holds, then the server outputs accept; otherwise, the outputs reject.

Compared to traditional public key-based cryptographic tools, ZKP is a more secure method in IoT with smaller computational requirements, which we summarized in Table 5. However, they may not be suitable for IoT since traditional ZKP schemes are usually not efficient. Hence, we explore the efficient, functional, and secure implementation of different applications of ZKP in IoT with anonymous communications. We will categorize the ZKP-based authentication in IoT by various networks and properties, and summarize it in Table 6. Furthermore, we summarize why ZKP works in IoT.

Table 5. Comparison between ZKP-based authentication and PKI-based authentication.

Scheme	Property	Decentralization	MIMA
	ZKP	✓	✓
PKI	CA-based	×	✓
	non-CA-based	✓	×

5.1. The Strengths of ZKP in IoT

Traditional ZKP schemes are usually not efficient. However, ZKP is still increasingly used in IoT because of its unique properties. Overall, ZKP has two major advantages that cause it to be an important technology to protect privacy.

The first reason is that ZKP has the property of *zero knowledge*. In traditional authentication schemes, the smart IoT devices must store large amounts of authentication data, which may put this data at risk. However, in ZKP, the verifier or other person will not learn anything from the interactive part, which can effectively protect data privacy. This enables ZKP to implement the following two properties.

- *Anonymity*. Aiming at concealing the real identities of users during communications, IoT needs to provide complete and mutual anonymity for each node. However, conventional proxy-based techniques fail to support authentication. Zero-knowledge of ZKP naturally enables anonymity and supports authentication. Furthermore, ZKP can be extended to anonymous communications, anonymous payments, and anonymous access.
- *Man-in-the-middle Resistance*. MIMA (Man-in-the-middle attack.) refers to an intruder that can establish independent connections and can arbitrarily access, modify, and relay messages between two parties without either party recognizing that the links between them have been compromised. ZKP binds the user's information and the key exchange data. When binding the proof, any attempts to modify the messages cannot pass the verification of legitimate users. Following this idea, ZKP-based schemes can also avoid forgery, password attacks, replay attacks, tracking, etc.

The second reason is that ZKP has a *relatively low overhead*. For example, if the symmetric cryptography is used to establish secure communication over insecure channels, the overhead of securely transmitting the symmetric keys is very high since the amount of IoT devices is very giant. On the other hand, public key infrastructure (PKI) needs high computational complexity. This is because, for the environment of IoT, most public key cryptosystems are not lightweight enough. ZKP is comparatively lightweight. It can effectively reduce computational complexity and communication complexity by combining them with other technologies.

- *Reduction in Computational Complexity*. In IoT devices, M-ZAS [54] is 3 times more efficient than GMW-ZKP and even 7 times more efficient than traditional authentication mechanisms because it has multiple individual graphs instead of a single one. Compared with the two ECDSA-based authentication schemes, TinyECC [55] and WM-ECC [56], TinyZKP [57] operates $1.9\times$ and $1.4\times$ faster and has 48% and 28% lower energy costs, respectively. BANZKP [58] combines ZKP and a commitment scheme. Compared to TinyZKP [57], it is 17 times more efficient in running time with 94.11% less energy.
- *Reduction in Communication Complexity*. The elliptic curve-based ZKP [59] has a smaller code. Moreover, the exchanged information is well suited to the technical specifications of the standard IEEE 802.15.4 scheme. For the authentication challenge, Walshe et al. [60] replaced the original ZKP-based hard problem with a Merkle tree structure that grows a challenge package with a minimum number of requirements. LiteZKP [61] reduces the energy consumption and latency of IoT edge-computing platforms by more than 55%.

Now, we compare ZKP-based authentication and PKI-based authentication in Table 5. There are two models in the Public Key Infrastructure (PKI): CA-based and non-CA-based. In CA-based authentication, a commonly trusted third party is required to ensure the validity of the binding of a user public key and their identity. However, this CA-based model is not suitable for decentralized environments. In non-CA-based authentication, users use their public keys as the pseudonyms. Further, the self-signed certificate is used to authenticate the reality of a peer's pseudonym. This technique can provide anonymity for vender and vendee in a "face-to-face" scenario. However, this technique cannot resist the MIMA. In short, ZKP obtains the trade-off between privacy protection and overhead.

5.2. Classification by Networks

5.2.1. Applications in Mobile Ad Hoc Networks

A mobile ad hoc network (MANET) is a multi-hop mobility peer-to-peer network consisting of from tens to hundreds of mobile devices that are dynamically networked using wireless communication methods. Mobile devices often do not have access to the network in many places due to their mobility. Therefore, a legitimate node with a network connection may wish to rent its connection to other legitimate devices. For this task, Martín-Fernández et al. [62] design a NIZK-based authentication for two devices to build a shared secret session key and exchange confidential data. In this work, a node can authenticate its own legitimacy to join another legitimate user's communication session by decrypting and verifying all of the commitments broadcast by another user. It can be concluded that the scheme [62] from the implementations is computationally faster compared to other related work.

5.2.2. Applications in Vehicular Networks

As a special type of MANET, the vehicle network is to achieve an efficient traffic management communication network between sensors, controls, and actuators within a vehicle connected in a complex mesh of point-to-point wires. The main goal of vehicle networks is to achieve efficient traffic management to prevent desirable conditions on the roads. However, the connected but malicious vehicles in the networks can send false traffic and vehicular data to the centralized traffic management system and its data center. In this case, the centralized traffic management system and its data center should have the ability to authenticate the data obtained from vehicular networks. This issue can be solved using Martín-Fernández et al.'s work [62] based on NIZK.

5.2.3. Applications in Wireless Sensors Networks

A wireless sensor network (WSN) is a framework of the network formed by organizing and combining tens of thousands of sensor nodes in a free-form manner through wireless communication technology. Its security includes WSN internal communication security and data security; the goal is to resist external intrusion and to ensure the node security and sensory data's confidentiality, integrity, authenticity, etc. Based on preloaded parameters in existing WSN models, the generated shared key designed by Martín-Fernández et al. [62] is exploited as a broadcast key for smart IoT devices. Walshe et al. [60] exploited the Merkle tree structure instead of ZKP for creating authentication challenges in WSN. The simulation results indicate that this approach is suitable for authentication in resource-constrained IoT environments.

5.2.4. Applications in Wireless Body Area Networks

A wireless body area network (WBAN) is a communication technology centered on the human body and composed of various network elements related to the human body. These elements include personal terminals, sensors distributed around and even inside the human body, and networking devices. It is mainly used for monitoring human sensor networks and human health, or for applications centered on cell phones or mobile devices. Due to the specificity of WBAN in healthcare applications, its security requirements are confidentiality,

and private information protection. A lightweight authentication scheme was proposed by Ma et al. [57] for WBAN, called TinyZKP. Compared to traditional ECDSA-based (Elliptic curve digital signature algorithm.) authentication schemes, the simulation results indicate that the performance of TinyZKP is better in terms of time cost and energy cost.

5.2.5. Applications in Crowdsourcing IoT

Crowdsourcing refers to the practice of a company or organization outsourcing work tasks previously performed by employees to non-specific (and often large) mass volunteers on a free and voluntary basis. Crowdsourcing IoT allows for remotely accessing information of all of these devices securely through a wireless channel by a home gateway node or a server that acts as a bridge between smart devices and the home users. A remote multi-factor authentication scheme was proposed by Liu et al. [63], which has three factors: identities, passwords, and biometrics of users. They achieve this goal with zero-knowledge proof based on a chaotic map-based computational Diffie–Hellman problem (CMCDHP), which has lower computational overhead and smaller key size. Moreover, the authors proved the strong forward security, which is more suitable in fifth generation mobile communication. Hence, this work is ideal for smart devices with limited power, as well as 5G technology.

5.3. Classification by Properties

5.3.1. Anonymity

Anonymity means that the communicating parties do not need each other to trust themselves by disclosing their identities. In the cloud-based radio over optical-fiber networks (C-RoFN), Yuan et al. [64] proposed an anonymous access system using ZKP for blockchain-based IoT devices. The operator computes the divided identity block data while the device evaluates the total digital identity using ZKP. This approach completes the device's anonymous access to IoT. With a smart contract-based ZKP, Bools et al. [61] present a framework for supporting multiple anonymous payments, called LiteZKP. In this work, Alice sends ETH to Bob using ZKP. Then, the verifier (smart contract) checks the condition without revealing the public key of Alice. Hence, it offered a fully anonymous system. Furthermore, to reduce the number of ZKP operations, LiteZKP used Merkle tree machines and integrates ZKP into an off-chain payment channel. Dwivedi et al. [8] also provide an efficient ZKP-based authentication system to realize the legitimate users' anonymity.

5.3.2. Decentralization

As IBM said, the extension of IoT is renovated from a trusted, costly, and centralized framework to a self-managed and self-regulating decentralized architecture [65]. Chuang et al. [54] proposed an authentication system (M-ZAS) that is not only lightweight but also highly adaptive and is based on multi-graph ZKP. Especially, compared to other centralized approaches, M-ZAS is more flexible for IoT without a centralized controller. It also provided higher performance, lower transmission, and better security protection than GMW-ZKP and other traditional authentication mechanisms do. Furthermore, ZKP-based authentication is used in blockchain-based IoT. Li et al. [66] proposed a decentralized and location-aware architecture in privacy-preserving blockchain-based traffic management systems. The traveling vehicle sends the messages encrypted by a NIZK-based range proof scheme to the gateway to verify its information. The gateway is for the traveling vehicle logs into an entering traffic management system. For real-time traffic management, the experiment results indicate that this method is more effective and feasible. Guo et al. [67] used ZKP to realize the identity verification mechanism in the blockchain environment.

5.3.3. Post Quantum

Quantum algorithms, such as the Shor algorithm [68], will solve hard problems such as discrete logarithm and factorization problems in quantum computers in polynomial time. Therefore, traditional public key cryptosystems such as RSA, DSA, and ECDSA will become

insecure for post-quantum. Akleyek et al. [69] propose a lattice-based authentication scheme for IoT technologies such as RFID systems, which also satisfies the zero-knowledge property.

Table 6. ZKP-based Authentication in IoT.

Scheme	Year	Features
[70]	2014	M2M
[57]	2014	WBAN
[62]	2016	MANET
[54]	2017	Decentration
[60]	2019	WSN
[63]	2020	Crowdsourcing IoT
[66]	2020	Decentration; Traffic management
[64]	2021	Anonymity; Decentration; Access control
[71]	2021	WSN; Improving efficiency
[8]	2021	Anonymity
[61]	2021	Anonymity; Decentration; Blockchain
[69]	2022	Post-quantum
[67]	2022	Decentration; Fabric Blockchain

6. Challenges and Future Research Directions

Some eternal issues of ZKP in IoT are discussed here: security and efficiency. In addition, we outline several possible further research directions in Table 7.

Table 7. Summary of future direction in ZKP-based IoT.

Direction	Requirements	Challenges
5G	Reliable resilience, low latency, highly scalable, and high data rates with fine-grained networks	Data privacy
Decentralization	No third-party key distribution platform or trusted and fair management platform	Limited memory resource
Post-quantum	Resist quantum computing attacks	Lightweight algorithm

6.1. The Challenge of ZKP in IoT

- *Lighter.* The existing ZKP models are continuously optimized to adapt to complex IoT network environments. However, with the advent of the 5G era, the demand for real-time communication has increased, such as in the live broadcasting industry. Lighter algorithms are always worth investigating and ZKP still has space for optimization. For example, the scheme of Walshe et al. [60] provided optimal cryptographic methods for obtaining node data while verifying the Merkle tree's creation. We can choose a more efficient mathematical structure to improve the efficiency, such as lattice.
- *Safer.* The security of ZKP in IoT depends on mathematically hard assumptions, including graph isomorphism and discrete logarithm. Hence, ZKP can resist main attacks, such as MIMA, forgery, password attacks, replay attacks, tracking, etc. However, there are some security holes to consider. All traditional secure transport layer schemes, such as TLS, are vulnerable to cross-protocol attacks if the pre-shared key exploits the Diffie–Hellman parameters [72]. There may be some backdoors in IoT operating systems that could lead to some over-privileged nodes accessing sensitive data at any time [73]. How to use ZKP to meet higher security requirements is still worth considering.

6.2. Further Research Direction

6.2.1. ZKP in 5G-IoT

The 5th generation mobile communication technology (5G) is a new generation of broadband mobile communication technology with high speed, low latency, and large connectivity, and 5G communication facilities are the network infrastructure to realize the interconnection of people, machines, and things. In 5G, billions of smart IoT devices can interact and share data without any assistance from humans. Much research work has been performed on the challenges of 5G IoT, including reliable resilience, low latency, highly scalable, and high data rates using fine-grained networks [74]. The security of various 5G-IoT systems is very complicated. The designers must consider both remote software intrusion and local device intrusion. It is worth studying how ZKP is applied to 5G-IoT to protect data privacy.

6.2.2. ZKP in Decentralized IoT

Decentralization refers to a system with a large number of nodes distributed where each node has a high degree of autonomy. There is no third-party key distribution platform or a trusted and fair management platform in blockchain-based IoT. We call it the decentralized IoT, which has high efficiency in processing without the limitations of third-party centrality. However, most of these efforts do not take into account threat traceability across the different endpoint lifecycles of the IoT [75]. Thus, in the cycle of these terminals, ZKP can implement effective threat tracking to avoid unnecessary security and privacy leaks when deploying IoT devices.

Furthermore, Wu et al. [76] describe a distributed zero-knowledge proof system (DIZK) that distributes the generation of a ZKP across multiple machines. Traditional ZKP systems are “monolithic”, so they are limited by the memory resources of a single machine, which is not suitable for decentralized IoT. At the same time, traditional ZKP systems are limited by a single machine’s memory resources, which is not suitable for the decentralized IoT. The combination of distributed ZKP and distributed IoT is an interesting direction.

6.2.3. ZKP in Post-Quantum IoT

Quantum computation greatly threatens public-key encryption systems, such as elliptic curve cryptography and Diffie–Hellman. These public key cryptographic algorithms are the key factors for the construction of ZKP models in IoT. The restrictions of IoT devices involving intensive mathematical computations require a large number of computational resources, which poses a related challenge to the development of IoT [77]. To date, code-based [78], super-singular elliptic curve isogeny [79], multivariate [80], lattice-based [81], and hybrid schemes [82] are five important types of post-quantum algorithms. Since latticed-based ZKP [41] is an effective post-quantum algorithm, it is worth researching efficient and secure ZKP-based IoT that holds the overhead of storing and manipulating large ciphertexts and large keys.

7. Conclusions

No doubt, IoT plays an important role in the future of the digital economy era. Unfortunately, user privacy is threatened due to resource-constrained devices and networks. Although the issues of the privacy and security of IoT have grown significantly in recent years; the zero-knowledge proofs (ZKP) system used in IoT still attracts increasing amounts of attention because of the unique properties of ZKP. In this paper, we present a summary of the security issues for the IoT, and then discuss the development process and advantages of ZKP-based authentication in IoT in detail. Finally, we propose a lighter and safer challenge in ZKP. Moreover, we introduced future development directions including 5G, decentralization, and post-quantum in IoT.

Author Contributions: Conceptualization, Y.J.; methodology, Y.J.; validation, Z.C.; formal analysis, Z.C.; investigation, X.S.; supervision, Z.C. and L.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by Zhejiang Province Public Welfare Technology Application Research, grant number LGF22F020001.

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

References

- Goldwasser, S.; Micali, S.; Rackoff, C. The Knowledge Complexity of Interactive Proof Systems. *SIAM J. Comput.* **1989**, *18*, 186–208. [\[CrossRef\]](#)
- Kumar, J.S.; Patel, D.R. A survey on internet of things: Security and privacy issues. *Int. J. Comput. Appl.* **2014**, *90*, 20–26.
- Yu, S.; Ren, K.; Lou, W. FDAC: Toward Fine-Grained Distributed Data Access Control in Wireless Sensor Networks. *IEEE Trans. Parallel Distrib. Syst.* **2011**, *22*, 673–686. [\[CrossRef\]](#)
- Picazo-Sanchez, P.; Tapiador, J.E.; Peris-Lopez, P.; Suarez-Tangil, G. Secure Publish-Subscribe Protocols for Heterogeneous Medical Wireless Body Area Networks. *Sensors* **2014**, *14*, 22619–22642. [\[CrossRef\]](#)
- Hu, C.; Zhang, J.; Wen, Q. An identity-based personal location system with protected privacy in IOT. In Proceedings of the 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology, Shenzhen, China, 28–30 October 2011; pp. 192–195.
- Liu, J.; Xiao, Y.; Chen, C.P. Internet of things' authentication and access control. *Int. J. Secur. Netw.* **2012**, *7*, 228–241. [\[CrossRef\]](#)
- Kalra, S.; Sood, S.K. Secure authentication scheme for IoT and cloud servers. *Pervasive Mob. Comput.* **2015**, *24*, 210–223. [\[CrossRef\]](#)
- Dwivedi, A.D.; Singh, R.; Ghosh, U.; Mukkamala, R.R.; Tolba, A.; Said, O. Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for Internet of Things. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *13*, 4639–4649. [\[CrossRef\]](#)
- Eschenauer, L.; Gligor, V.D. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS 2002, Washington, DC, USA, 18–22 November 2002; Atluri, V., Ed.; ACM: New York, NY, USA, 2002; pp. 41–47.
- Liu, D.; Ning, P. Establishing Pairwise Keys in Distributed Sensor Networks. In Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS '03, Washington, DC, USA, 27–30 October 2003; Association for Computing Machinery: New York, NY, USA, 2003; pp. 52–61.
- Du, W.; Deng, J.; Han, Y.S.; Varshney, P.K.; Katz, J.; Khalili, A. A Pairwise Key Predistribution Scheme for Wireless Sensor Networks. *ACM Trans. Inf. Syst. Secur.* **2005**, *8*, 228–258. [\[CrossRef\]](#)
- Venkatasubramanian, K.; Banerjee, A.; Gupta, S. EKG-based key agreement in Body Sensor Networks. In Proceedings of the IEEE INFOCOM Workshops 2008, Phoenix, AZ, USA, 13–18 April 2008; pp. 1–6.
- Bonetto, R.; Bui, N.; Lakkundi, V.; Olivereau, A.; Serbanati, A.; Rossi, M. Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. In Proceedings of the 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), San Francisco, CA, USA, 25–28 June 2012; pp. 1–7.
- Vučinić, M.; Tourancheau, B.; Rousseau, F.; Duda, A.; Damon, L.; Guizzetti, R. OSCAR: Object security architecture for the Internet of Things. *Ad Hoc Netw.* **2015**, *32*, 3–16.
- Ukil, A.; Bandyopadhyay, S.; Joseph, J.; Banahatti, V.; Lodha, S. Negotiation-Based Privacy Preservation Scheme in Internet of Things Platform. In Proceedings of the First International Conference on Security of Internet of Things, Kollam, India, 17–19 August 2012; Association for Computing Machinery: New York, NY, USA, 2012; pp. 75–84. [\[CrossRef\]](#)
- Doukas, C.; Maglogiannis, I.; Koufi, V.; Malamateniou, F.; Vassilacopoulos, G. Enabling data protection through PKI encryption in IoT m-Health devices. In Proceedings of the 2012 IEEE 12th International Conference on Bioinformatics Bioengineering (BIBE), Larnaca, Cyprus, 11–13 November 2012; pp. 25–29.
- Yi, X.; Bouguettaya, A.; Georgakopoulos, D.; Song, A.; Willemson, J. Privacy Protection for Wireless Medical Sensor Data. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 369–380. [\[CrossRef\]](#)
- Şimşek, M.; Şentürk, A. Fast and lightweight detection and filtering method for low-rate TCP targeted distributed denial of service (LDDoS) attacks. *Int. J. Commun. Syst.* **2018**, *31*, e3823. [\[CrossRef\]](#)
- Savaşçı Şen, S.; Cicioğlu, M.; Çalhan, A. IoT-based GPS assisted surveillance system with inter-WBAN geographic routing for pandemic situations. *J. Biomed. Inform.* **2021**, *116*, 103731. [\[CrossRef\]](#)
- Turkyilmaz, Y.; Senturk, A.; Bayrakdar, M.E. Employing machine learning based malicious signal detection for cognitive radio networks. *Concurr. Comput. Pract. Exp.* **2023**, *35*, e7457. [\[CrossRef\]](#)
- Jiang, H.; Shen, F.; Chen, S.; Li, K.C.; Jeong, Y.S. A secure and scalable storage system for aggregate data in IoT. *Future Gener. Comput. Syst.* **2015**, *49*, 133–141. [\[CrossRef\]](#)
- Kim, T.H.; Ramos, C.; Mohammed, S. Smart city and IoT. *Future Gener. Comput. Syst.* **2017**, *76*, 159–162. [\[CrossRef\]](#)
- Chandrakar, P.; Sinha, S.; Ali, R. Cloud-based authenticated protocol for healthcare monitoring system. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 3431–3447. [\[CrossRef\]](#)

24. Malik, H.; Zatar, W. Agent based routing approach to support structural health monitoring-informed, intelligent transportation system. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 1031–1043. [\[CrossRef\]](#)
25. Melis, A.; Prandini, M.; Sartori, L.; Callegati, F. Public transportation, IoT, trust and urban habits. In Proceedings of the International Conference on Internet Science, Florence, Italy, 12–14 September 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 318–325.
26. Raj, J.S.; Ananthi, J.V. Automation using IoT in greenhouse environment. *J. Inf. Technol.* **2019**, *1*, 38–47.
27. Jurcut, A.D.; Ranaweera, P.; Xu, L. Introduction to IoT Security. In *IoT Security: Advances in Authentication*; Wiley: Hoboken, NJ, USA, 2020; pp. 27–64.
28. Kim, H.; Lee, E.A. Authentication and Authorization for the Internet of Things. *IT Prof.* **2017**, *19*, 27–33. [\[CrossRef\]](#)
29. Höglund, J.; Lindemer, S.; Furuheid, M.; Raza, S. PKI4IoT: Towards public key infrastructure for the Internet of Things. *Comput. Secur.* **2020**, *89*, 101658. [\[CrossRef\]](#)
30. Marino, F.; Moiso, C.; Petracca, M. PKIoT: A public key infrastructure for the Internet of Things. *Trans. Emerg. Telecommun. Technol.* **2019**, *30*, e3681. [\[CrossRef\]](#)
31. Goldreich, O.; Micali, S.; Wigderson, A. Proofs that Yield Nothing However, Their Validity for All Languages in NP Have Zero-Knowledge Proof Systems. *J. ACM* **1991**, *38*, 691–729. [\[CrossRef\]](#)
32. Blum, M.; Feldman, P.; Micali, S. Non-Interactive Zero-Knowledge and Its Applications (Extended Abstract). In Proceedings of the 20th Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, 2–4 May 1988; Simon, J., Ed.; ACM: New York, NY, USA, 1988; pp. 103–112.
33. Groth, J.; Kohlweiss, M.; Maller, M.; Meiklejohn, S.; Miers, I. Updatable and Universal Common Reference Strings with Applications to zk-SNARKs. In Proceedings of the Advances in Cryptology—CRYPTO 2018, Santa Barbara, CA, USA, 19–23 August 2018; Shacham, H., Boldyreva, A., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 698–728.
34. Wahby, R.S.; Tzialla, I.; Shelat, A.; Thaler, J.; Walfish, M. Doubly-Efficient zkSNARKs Without Trusted Setup. In Proceedings of the 2018 IEEE Symposium on Security and Privacy, SP 2018, San Francisco, CA, USA, 21–23 May 2018; pp. 926–943.
35. Katz, J.; Kolesnikov, V.; Wang, X. Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 525–537.
36. Bünz, B.; Bootle, J.; Boneh, D.; Poelstra, A.; Wuille, P.; Maxwell, G. Bulletproofs: Short Proofs for Confidential Transactions and More. In Proceedings of the 2018 IEEE Symposium on Security and Privacy, SP, San Francisco, CA, USA, 20–24 May 2018; pp. 315–334.
37. Hoffmann, M.; Kloof, M.; Rupp, A. Efficient Zero-Knowledge Arguments in the Discrete Log Setting, Revisited. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 2093–2110.
38. Xie, T.; Zhang, J.; Zhang, Y.; Papamanthou, C.; Song, D. Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation. In Proceedings of the Advances in Cryptology—CRYPTO 2019—39th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2019; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11694, pp. 733–764.
39. Ben-Sasson, E.; Bentov, I.; Horesh, Y.; Riabzev, M. Scalable Zero Knowledge with No Trusted Setup. In Proceedings of the Advances in Cryptology—CRYPTO 2019—39th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2019; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11694, pp. 701–732.
40. Ben-Sasson, E.; Chiesa, A.; Riabzev, M.; Spooner, N.; Virza, M.; Ward, N.P. Aurora: Transparent Succinct Arguments for R1CS. In Proceedings of the Advances in Cryptology—EUROCRYPT 2019—38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, 19–23 May 2019; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11476, pp. 103–128.
41. Esgin, M.F.; Steinfeld, R.; Liu, J.K.; Liu, D. Lattice-Based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications. In Proceedings of the Advances in Cryptology—CRYPTO 2019—39th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2019; Boldyreva, A., Micciancio, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11692; pp. 115–146.
42. Yang, R.; Au, M.H.; Zhang, Z.; Xu, Q.; Yu, Z.; Whyte, W. Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications. In Proceedings of the Advances in Cryptology—CRYPTO 2019, Santa Barbara, CA, USA, 18–22 August 2019; Springer International Publishing: Cham, Switzerland, 2019; pp. 147–175.
43. Bootle, J.; Lyubashevsky, V.; Seiler, G. Algebraic Techniques for Short(er) Exact Lattice-Based Zero-Knowledge Proofs. In Proceedings of the Advances in Cryptology—CRYPTO 2019—39th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2019; Boldyreva, A., Micciancio, D., Eds.; Springer: Berlin/Heidelberg, German, 2019; Volume 11692, pp. 176–202. [\[CrossRef\]](#)
44. Daza, V.; Ràfols, C.; Zacharakis, A. Updateable Inner Product Argument with Logarithmic Verifier and Applications. In Proceedings of the Public-Key Cryptography—PKC 2020, Edinburgh, UK, 4–7 May 2020; Springer International Publishing: Cham, Switzerland, 2020; pp. 527–557.
45. Setty, S.T.V. Spartan: Efficient and General-Purpose zkSNARKs Without Trusted Setup. In Proceedings of the Advances in Cryptology—CRYPTO 2020—40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, 17–21 August 2020; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12172, pp. 704–737.

46. Zhang, J.; Xie, T.; Zhang, Y.; Song, D. Transparent Polynomial Delegation and Its Applications to Zero Knowledge Proof. In Proceedings of the 2020 IEEE Symposium on Security and Privacy, SP, San Francisco, CA, USA, 18–21 May 2020; pp. 859–876.
47. Bhadauria, R.; Fang, Z.; Hazay, C.; Venkitasubramaniam, M.; Xie, T.; Zhang, Y. Liger++: A New Optimized Sublinear IOP. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security CCS '20, Virtual, 9–13 November 2020; pp. 2025–2038.
48. Lyubashevsky, V.; Nguyen, N.K.; Seiler, G. Practical Lattice-Based Zero-Knowledge Proofs for Integer Relations. In Proceedings of the CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual, 9–13 November 2020; pp. 1051–1070.
49. Gvili, Y.; Scheffler, S.; Varia, M. BooLigero: Improved Sublinear Zero Knowledge Proofs for Boolean Circuits. In Proceedings of the Financial Cryptography and Data Security—25th International Conference, FC 2021, Virtual, 1–5 March 2021; Springer: Berlin/Heidelberg, Germany, 2021; Volume 12674, pp. 476–496.
50. de Saint Guilhem, C.D.; Orsini, E.; Tanguy, T. Limbo: Efficient Zero-knowledge MPCitH-based Arguments. In Proceedings of the CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual, 15–19 November 2021; pp. 3022–3036.
51. Zhang, J.; Liu, T.; Wang, W.; Zhang, Y.; Song, D.; Xie, X.; Zhang, Y. Doubly Efficient Interactive Proofs for General Arithmetic Circuits with Linear Prover Time. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual, 15–19 November 2021; pp. 159–177.
52. Lyubashevsky, V.; Nguyen, N.K.; Plançon, M. Lattice-Based Zero-Knowledge Proofs and Applications: Shorter, Simpler, and More General. In Proceedings of the Advances in Cryptology—CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, 15–18 August 2022; p. 284.
53. Implementing Zero-Knowledge Authentication with Zero Knowledge (ZKA_wzk). Available online: <http://hydra.azilian.net/Papers/Zero-knowledge-protocol.pdf> (accessed on 20 July 2022).
54. Chuang, I.H.; Guo, B.J.; Tsai, J.S.; Kuo, Y.H. Multi-graph Zero-knowledge-based authentication system in Internet of Things. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 22–25 May 2017; pp. 1–6.
55. Wang, W.; Cui, Y.; Chen, T. Design and implementation of an ECDSA-based identity authentication protocol on WSN. In Proceedings of the 2009 3rd IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, Beijing, China, 27–29 October 2009; pp. 1202–1205.
56. Wang, H.; Sheng, B.; Tan, C.C.; Li, Q. Public-key based access control in sensor network. *Wirel. Netw.* **2011**, *17*, 1217–1234. [\[CrossRef\]](#)
57. Ma, L.; Ge, Y.; Zhu, Y. TinyZKP: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks. *Wirel. Pers. Commun.* **2014**, *77*, 1077–1090. [\[CrossRef\]](#)
58. Khernane, N.; Potop-Butucaru, M.; Chaudet, C. BANZKP: A Secure Authentication Scheme Using Zero Knowledge Proof for WBANs. In Proceedings of the 2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Brasilia, Brazil, 10–13 October 2016; pp. 307–315.
59. Chatzigiannakis, I.; Pyrgelis, A.; Spirakis, P.G.; Stamatiou, Y.C. Elliptic Curve Based Zero Knowledge Proofs and Their Applicability on Resource Constrained Devices. In Proceedings of the 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia, Spain, 17–22 October 2011; pp. 715–720.
60. Walshe, M.; Epiphaniou, G.; Al-Khateeb, H.; Hammoudeh, M.; Katos, V.; Dehghantanha, A. Non-interactive zero knowledge proofs for the authentication of IoT devices in reduced connectivity environments. *Ad Hoc Netw.* **2019**, *95*, 101988. [\[CrossRef\]](#)
61. Boo, E.; Kim, J.; Ko, J. LiteZKP: Lightning Zero-Knowledge Proof-Based Blockchains for IoT and Edge Platforms. *IEEE Syst. J.* **2021**, *16*, 112–123. [\[CrossRef\]](#)
62. Martín-Fernández, F.; Caballero-Gil, P.; Caballero-Gil, C. Authentication Based on Non-Interactive Zero-Knowledge Proofs for the Internet of Things. *Sensors* **2016**, *16*, 75. [\[CrossRef\]](#)
63. Liu, W.; Wang, X.; Peng, W. Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things. *IEEE Access* **2020**, *8*, 8754–8767. [\[CrossRef\]](#)
64. Yuan, J.; Yang, H.; Dong, S.; Yao, Q.; Jiao, L.; Zhang, J. Demonstration of Blockchain-based IoT Devices Anonymous Access Network Using Zero-knowledge Proof. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 15–19 June 2020; pp. 1607–1609.
65. Brody, P.; Pureswaran, V. Device democracy: Saving the future of the Internet of Things. 2014. Available online: [http://refhub.elsevier.com/S1084-8045\(18\)30347-3/sref27](http://refhub.elsevier.com/S1084-8045(18)30347-3/sref27) (accessed on 15 July 2015).
66. Li, W.; Guo, H.; Nejad, M.; Shen, C.C. Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach. *IEEE Access* **2020**, *8*, 181733–181743. [\[CrossRef\]](#)
67. Guo, H.; Cheng, J.; Wang, J.; Chen, T.; Yuan, Y.; Li, H.; Sheng, V.S. IoT Data Blockchain-Based Transaction Model Using Zero-Knowledge Proofs and Proxy Re-encryption. In Proceedings of the Artificial Intelligence and Security, Los Angeles, CA, USA, 11 November 2022; pp. 573–586.
68. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [\[CrossRef\]](#)
69. Akleylek, S.; Soysaldi, M. A new lattice-based authentication scheme for IoT. *J. Inf. Secur. Appl.* **2022**, *64*, 103053. [\[CrossRef\]](#)

70. Flood, P.; Schukat, M. Peer to peer authentication for small embedded systems: A zero-knowledge-based approach to security for the Internet of Things. In Proceedings of the 10th International Conference on Digital Technologies 2014, Zilina, Slovakia, 9–11 July 2014; pp. 68–72.
71. Soewito, B.; Marcellinus, Y. IoT security system with modified Zero Knowledge Proof algorithm for authentication. *Egypt. Inform. J.* **2021**, *22*, 269–276. [[CrossRef](#)]
72. Mavrogiannopoulos, N.; Vercouteren, F.; Velichkov, V.; Preneel, B. A Cross-Protocol Attack on the TLS Protocol. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, Raleigh, NC, USA, 16–18 October 2012; Association for Computing Machinery: New York, NY, USA, 2012; pp. 62–72.
73. Hashemi, S.; Zarei, M. Internet of Things backdoors: Resource management issues, security challenges, and detection methods. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4142.
74. Li, S.; Xu, L.D.; Zhao, S. 5G Internet of Things: A survey. *J. Ind. Inf. Integr.* **2018**, *10*, 1–9. [[CrossRef](#)]
75. Qian, Y.; Jiang, Y.; Chen, J.; Zhang, Y.; Song, J.; Zhou, M.; Pustišek, M. Towards decentralized IoT security enhancement: A blockchain approach. *Comput. Electr. Eng.* **2018**, *72*, 266–273. [[CrossRef](#)]
76. Wu, H.; Zheng, W.; Chiesa, A.; Popa, R.A.; Stoica, I. DIZK: A Distributed Zero Knowledge Proof System. In Proceedings of the 27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, 15–17 August 2018; pp. 675–692.
77. Fernández-Caramés, T.M. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 6457–6480. [[CrossRef](#)]
78. McEliece, R.J. A public-key cryptosystem based on algebraic. *Coding Thv* **1978**, *4244*, 114–116.
79. Rostovtsev, A.; Stolbunov, A. Public-Key Cryptosystem Based on Isogenies. Available online: <https://eprint.iacr.org/2006/145> (accessed on 20 August 2022).
80. Ding, J.; Petzoldt, A.; Wang, L. The Cubic Simple Matrix Encryption Scheme. In Proceedings of the Post-Quantum Cryptography—6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, 1–3 October 2014; Mosca, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8772, pp. 76–87.
81. Peikert, C. Lattice Cryptography for the Internet. In Proceedings of the Post-Quantum Cryptography—6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, 1–3 October 2014; Mosca, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8772, pp. 197–219.
82. Google Blog on Google’s Experiments with a Hybrid Cryptosystem. 2016. Available online: <https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html> (accessed on 7 July 2016).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.