

Review

Cryptography-Based Security Authentication and Privacy Preservation of Cyber-Physical Power Systems: An Overview

Cheng Jiang ^{1,2} , Jianyong Bi ¹, Huiqun Yu ^{1,*} , Mi Wen ¹, Lei Wu ³ and Rolf Findeisen ⁴

¹ Department of Artificial Intelligence, Shanghai University of Electric Power, Shanghai 201306, China; c.jiang@shiep.edu.cn (C.J.); jianyongbi@mail.shiep.edu.cn (J.B.); miwen@shiep.edu.cn (M.W.)

² Shanghai Key Laboratory of Power Station Automation Technology, Department of Intelligent Artificial, Shanghai University of Electric Power, Shanghai 201306, China

³ Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ 07030, USA; lei.wu@stevens.edu

⁴ Control and Cyber-Physical Systems Laboratory, TU Darmstadt, 64227 Darmstadt, Germany; rolf.findeisen@iat.tu-darmstadt.de

* Correspondence: yuhuiqun@shiep.edu.cn

Abstract

Cyber-physical power systems (CPPSs) are a crucial component of smart grids, integrating physical power systems with advanced information and communication technologies to achieve efficient, reliable, and intelligent energy management and control. However, with the widespread deployment of information technology, CPPSs face increasingly severe security threats and privacy protection challenges, such as data leakage, identity forgery, and impersonation, which can compromise the secure and stable operation of CPPSs. To counter these threats and protect privacy, cryptographic technique is developed to provide fundamental and powerful tools, supporting secure authentication, data integrity checking, privacy preservation, and trusted communication between connected devices in CPPSs. We systematically review the research progress on security authentication and privacy protection in CPPSs from a cryptographic perspective. Our survey analyzes the major security threats faced by CPPSs, along with the impact of various attacks on system data. We explore mainstream cryptographic algorithms, including digital signatures, key agreement protocols, signcryption authentication, homomorphic encryption, and blockchain-based security mechanisms that are capable of resisting cyber attacks and ensuring reliable decision-making and control in CPPSs. This work also provides the trends and challenges regarding the intersection of cryptography and networked control, blockchain scalability, and convergence of cryptography and artificial intelligence in CPPSs.

Keywords: cyber-physical power systems; cryptography; security authentication; privacy preservation



Academic Editor: Panayiotis Kotzanikolaou

Received: 6 June 2026

Revised: 14 July 2026

Accepted: 21 July 2026

Published: 22 July 2026

Copyright: © 2026 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 \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Power system, as a critical national infrastructure, is not only related to national economic security but is also closely connected to the livelihoods and social stability of people. The accelerated application of next-generation information and communication technologies in traditional power systems is driving the transition of conventional power systems into cyber-physical power systems (CPPSs) [1,2]. This deep integration of physical power grids with the information space enhances the observability and controllability of the power systems, improving their economic efficiency and reliability [3]. With the

widespread application of emerging digital technologies like 5G, artificial intelligence, and big data, CPPSs enable the sharing and collaborative operation of massive data across the source-network-load-storage sections. This has led to the continuous emergence of new business scenarios within the system, which has made the security boundary of power grids increasingly blurred. As the security boundary of CPPSs continues to expand and extend, in addition to the physical security issues caused by traditional component and equipment failures, the increasing penetration of communication networks into CPPSs has made the system structure more complex and its operational environment more open. CPPSs are highly vulnerable to cybersecurity risks (for example, impersonation, manipulation, and eavesdropping attacks) that originate in information systems [4,5].

In the face of huge economic benefits and low attack costs, malicious adversaries exploit the security vulnerabilities present in CPPSs to launch attacks, mainly destroying power data confidentiality, authenticity, integrity, and privacy. These security attributes manifest critically in real-world power operations.

- Confidentiality ensures that data is accessible only to authorized entities and protected from unauthorized interception, disclosure, or eavesdropping. Breaches of confidentiality, such as eavesdropping on communication links, infiltrating databases to steal grid topology, real-time load/generation statistics, can expose system vulnerabilities, which enables complex follow-up attacks, or provides unfair market advantages to adversaries.
- Authenticity ensures that data sources (e.g., sensor readings, control commands, user consumption reports) are genuine and authorized. Attacks compromising authenticity, like spoofing legitimate devices or injecting false data, can lead to catastrophic operational decisions based on fabricated states.
- Integrity guarantees that data remains unaltered during transmission or storage. Tampering with critical operational data (e.g., altering line flow measurements, modifying generator setpoints, or falsifying market bids) can directly destabilize the grid or cause economic losses.
- Privacy focuses on the association between data and identifiable individuals or entities. Identity privacy prevents the linkage of specific data points (e.g., energy usage patterns) to residential users, industrial facilities, or personnel. Unauthorized linkage can reveal personal habits, business activities, or operational schedules. Note that anonymized operational data not linked to any identity falls under confidentiality, not privacy. When privacy is violated, attackers may profile users, conduct social engineering, or target key personnel, further undermining the overall security posture.

These security features are interrelated and work together to maintain data security. When these security features are compromised, the deep integration of power grids and information networks allows the impact of attacks to easily penetrate the power system itself, compromising its safe and stable operation, and potentially triggering major security incidents [6]. For example, in 2019, the core computer systems of Venezuela's Guri Hydroelectric power plant and its connected control hub in the capital suffered malicious cyber attacks. This resulted in power outages across 21 out of 23 states, affecting over 90% of administrative regions, including the capital, Caracas. Nearly 30 million people were impacted, causing severe repercussions for the country's economy, society, and politics.

In the face of cyber threats, traditional passive defense methods, such as intrusion detection and vulnerability patching, can no longer meet the security protection requirements of CPPSs. Active defense approaches capable of early detection and prediction of attacks are emerging as a critical solution. Recent reviews on intelligent detection techniques have systematically examined coordinated attack behaviors and cascaded failure patterns [7], providing a systematic framework for post-attack detection [8]. Proactive

detection methods have been developed to identify pre-attack anomalies and issue early warnings before full-scale attacks occur, with experimental validations demonstrating high detection accuracy and practical lead times [9,10]. Unlike detection-based approaches that primarily identify anomalies after or during the early stages of an attack, cryptographic methods provide intrinsic security protection for data itself through encryption and authentication mechanisms, safeguarding confidentiality, integrity, and authenticity from the source, and thus represent a more fundamental proactive defense strategy. Cryptography-based security authentication and privacy preservation, as an effective method of active defense, has attracted widespread attention from scholars worldwide. This approach focuses on identity-based security, assigning logical identities to devices/users in network communications, and performing authentication, authorization, and encryption for all access requests. It can effectively resist cyber attacks and protect privacy [11]. Therefore, research on cryptography-based secure identity authentication and privacy-preserving methods for power equipment to improve system security from the source of device access is of great significance.

CPPS data security and privacy preservation approaches have been intensively presented in the past decade, and review papers on these methods are summarized in Table 1. Nevertheless, most of these review papers [12–17] focus on a single aspect of security authentication and privacy preservation. Featuring verifiable theoretical security and flexible privacy computing functions, cryptography is widely studied and deployed to defend CPPS data transmission against eavesdropping, tampering and identity forgery threats. Thus, it is necessary to perform an in-depth analysis by considering all aspects of data confidentiality, authenticity, integrity, and privacy of data of the CPPSs under cyber attacks.

Table 1. A review of the published literature related to security authentication and privacy preservation.

References	Topics	Contents
[12]	Security authentication	Analysis of authentication of smart grid focusing on authenticity and integrity
[13]		Analysis of authentication and key agreement of smart grid aiming at authenticity and integrity
[14]		Analysis of post-quantum cryptographic authentication of smart grid to guarantee authenticity and integrity
[15]	Privacy preservation	Analysis of differential privacy method to protect data privacy
[16]		Analysis of differential privacy method and its application to protect smart grids' privacy
[17]		Analysis of aggregation method to protect privacy of smart meters
Ours	Security authentication and Privacy preservation	Analysis of cryptography-based security and privacy in CPPSs covering confidentiality authenticity integrity and privacy

By observing the research gap in existing literature reviews, this paper offers the following contributions:

- (1) This paper provides an analysis of cyber attacks in CPPS networks and an impact analysis of system data under cyber attacks, including data authenticity, integrity, and privacy.

- (2) This paper surveys cryptography-based security authentication approaches in single domain and among multidomains of CPPSs, focusing on the security aspects of data authenticity and integrity.
- (3) This paper compares cryptography-based privacy-preserving methods for CPPSs, focused on data privacy.
- (4) This paper discusses the research trends towards security authentication and preservation of CPPS privacy.

In this survey, we systematically review the state-of-the-art countermeasures for CPPS data security from the perspectives of four fundamental attributes: confidentiality, authenticity, integrity, and privacy. The structure of the rest of this paper is as follows. In Section 2, we introduce the security risk analysis of CPPS networks and the impact analyses of CPPS data under cyber attacks. Section 3 discusses cryptography-based security authentication methods, and Section 4 examines preservation of privacy from the point view of cryptography. Section 5 lays out the challenge issues. Finally, we draw our conclusions in Section 6. The key points of our survey are shown in Figure 1.

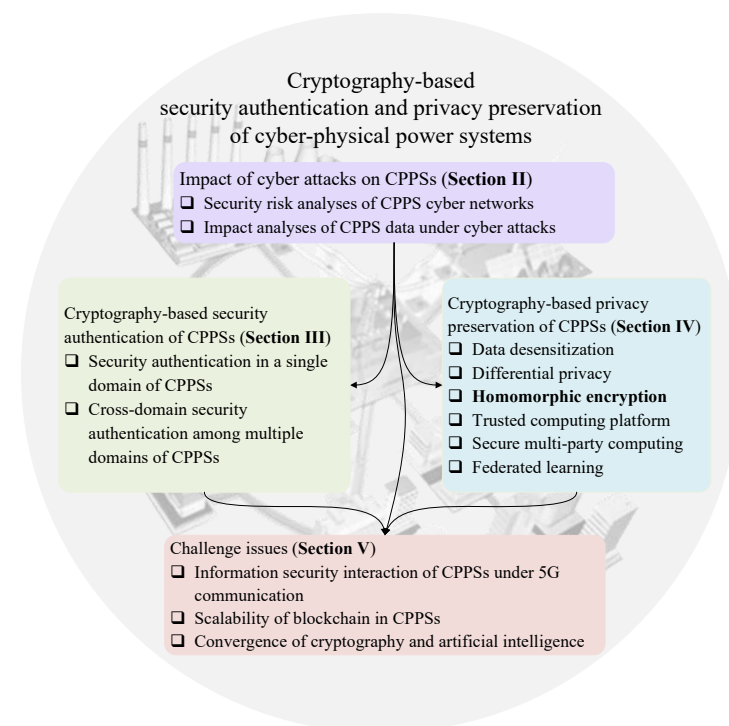


Figure 1. A taxonomy of key points of our survey on security authentication and privacy preservation for CPPSs.

2. Impact of Cyber Attacks on CPPSs

2.1. Cyber Attack Analyses in CPPSs

The control layer of CPPSs implements automatic control functions such as load frequency control, voltage control, and economic dispatch. It executes control commands from the monitoring center by implementing corresponding control strategies (e.g., adjusting generator power outputs). This layer processes massive volumes of sensitive data, including grid topology, power load data, equipment status information, and operational index. Once these data are subjected to malicious attacks, this can lead to severe consequences such as operational instability, decision-making errors, and market disruption in CPPSs [18]. Common data attacks include false data injection attack, data replay attack, and man-in-the-middle attack.

2.1.1. False Data Injection Attack

It represents an emerging threat vector, particularly targeting the deeply coupled cyber-physical nature of CPPSs [19]. By maliciously tampering with sensor measurements at the acquisition end and state estimation results at the control end, false data injection attacks destroy data integrity, causing physical system's operational state or erroneous control actions. Driven by advances in digital technology and evolving user demands, these systems exhibit characteristics of high complexity, extreme decentralization, and massive device data [20]. This creates a significantly larger potential attack surface for false data injection attack. False data injection attacks can inject false renewable generation outputs, electricity demands, or dispatch commands among specific nodes in the power system. This malicious data injection disrupts the stable grid integration and operation of renewable energy.

2.1.2. Data Replay Attack

In CPPSs, data replay attacks constitute a significant way of data forgery attack [21]. Attackers intercept and capture data packets, subsequently retransmitting previously received monitoring data to the target host. This aims to deceive the system, primarily undermining the data authenticity. With the integration of high-speed wireless communication technologies like 4G and 5G into CPPSs, the vast volumes of data generated by digital transformation become increasingly vulnerable to data replay attacks. Once an attacker successfully initiates a data replay attack and bypasses the authentication system, they could disrupt the operational state of the physical power infrastructure by repeatedly transmitting the same control commands [22]. Alternatively, by retransmitting sensed measurement data from the terminal side, they could prevent the dispatch and control master station from accurately assessing the normal operating state of the physical power system, ultimately compromising power system stability.

2.1.3. Man-in-the-Middle Attack

It constitutes an indirect intrusion strategy where an attacker covertly positions themselves within the network connection between two or more communicating terminals [23]. This enables the interception, eavesdropping, and potential tampering with data traversing the channel, compromising the confidentiality, authenticity, integrity, and privacy of data. Distinct from other cyber attack methodologies, man-in-the-middle attacks can decode communication protocols to disguise the attacked device, resulting in significantly enhanced stealth and greater difficulty in detection.

In CPPSs, attackers exploiting man-in-the-middle attacks can perform identity spoofing or certificate forgery. This allows them to impersonate legitimate nodes in the power grid. By intercepting communications and subsequently injecting false critical information towards other nodes, attackers can disrupt the normal operation of the power system. This interference will lead to severe consequences such as supply-demand imbalance, market disorder, and equipment damage.

2.2. Security Risk Analyses of CPPS Cyber Networks

As an important part of the power system, the cyber security risks of CPPSs should not be ignored. CPPSs mainly use public wireless networks, 230 MHz private wireless networks, private fiber optic networks, power carriers, RS-485 bus and other communication modes to interact, which brings convenience and also introduces potential security risks. Due to the vulnerability of communication protocols or physical damage, open CPPSs are exposed to security threats such as data leakage, tampering, denial of service, etc., which may even lead to power system paralysis in severe cases. Table 2 provides a detailed analysis

of the main security risks faced by CPPSs. It shows that the continuous expansion of communication networks within CPPS has led to increasingly complex system architectures and progressively open operating environments, rendering them highly vulnerable to cyber security risks from information systems, and further impacting power data.

Table 2. Security risk analyses of CPPS cyber networks.

Communication Modes	Cyber Security Risks
Public wireless network	(1) The public wireless network itself: It adopts TCP/IP with inherent IP network vulnerabilities, vulnerable to DoS attacks and virus infections. (2) Extranet: It threatens power collection/control terminals and intranet preamplifiers. DDoS attacks, data theft and false control injection may occur; extranet viruses cause communication blockage. (3) Intranet: Internal users may threaten wireless collection/control terminals. DDoS and viruses on intranet-extranet links lead to link blockage.
230 MHz private wireless network	(1) Channel defects: It is an open transparent network and highly vulnerable to cyber attacks. (2) Identity forgery: No identity authentication mechanism exists, the system faces identity forgery risks. (3) Information eavesdropping: Due to channel defects, attackers build illegal stations to fully eavesdrop transmission data for subsequent attacks. (4) Replay Attack: In the absence of security measures in the current 230 MHz private wireless network, intercepted messages can be retransmitted at any time with no time limit. (5) Information tampering: It is a broadcast network, which may suffer from information tampering.
Private fiber optic network	It owns high security attributes against malicious attacks. Compared with other channels, private fiber optics hold prominent security advantages.
Power carrier	Using power lines as channels, it faces risks of data interception, tampering and deletion.
RS485 bus	There may be security risks during RS485 channel data transmission, including defects in the channel itself, channel corruption, illegal access, data tampering, interception, and deletion.

2.3. Impact Analyses of CPPS Data Under Cyber Attacks

CPPSs span multiple stages, including power generation, transmission, distribution, and consumption, as shown in Figure 2, each stage relying heavily on a large number of sensors, actuators, and communication modules. Furthermore, CPPSs are highly susceptible to multilayer (i.e., power, network, and control layers), multipoint (i.e., devices or nodes in power generation, transmission, distribution, and consumption), and multistyle (e.g., tampering, impersonation, eavesdropping, and man-in-the-middle) cyber attacks due to their complex multi-layer structure and open communication networks [24], which disrupts data transmission and control commands.

In the power generation stage, adversaries can manipulate control data from local excitation or speed regulation devices, causing deviations from stable operating conditions. More severe consequences arise when wide-area control systems are targeted, such as by altering collected data or forging control commands. These attacks can disrupt economic dispatch [25], load frequency control, and overall optimality of the system, potentially leading to instability. In the transmission stage, due to the critical role of supervisory control and data acquisition/energy management system and wide area measurement system, malicious adversaries can manipulate equipment statuses or transmit false measurement data, mislead power flow dispatch, impair equipment protection functions, or even trigger large-scale faults. The distribution stage is equally vulnerable; for example, advanced metering infrastructure can be attacked and communication modules in distributed energy systems and distribution management systems are often subjected to data manipulation, impersonation, and man-in-the-middle attacks that can undermine the stability of renewable energy integration and the reliability of scheduling. Finally, in the consumption stage,

as the terminal part of the system, home area networks face risks such as a modified real-time electricity price and stolen user privacy data, directly threatening the accuracy of electricity metering and user financial interests. Therefore, the openness and complexity of CPPSs make them prime targets for attackers, destroying data essential security properties, such as confidentiality, authenticity, integrity, and privacy.

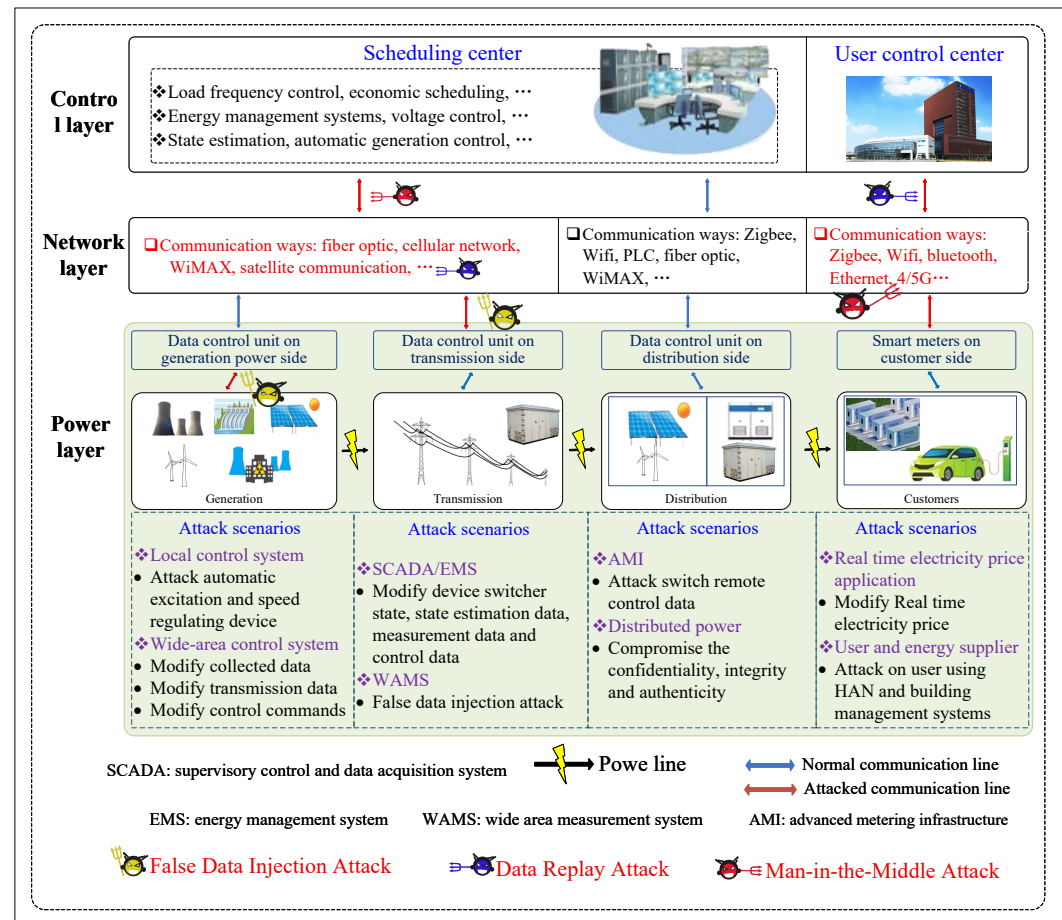


Figure 2. Attack scenarios in CPPSs.

When data is attacked, i.e., authenticity, integrity, or privacy is destroyed, the deep integration of the power and network layers exacerbates the propagation of attack impacts, resulting in system-wide consequences and further posing severe threats to the safe and stable operation of CPPSs. Cyber attacks essentially destroy core security properties of data, including confidentiality, authenticity, integrity and privacy. When corrupted data participates in the calculation, analysis and decision-making processes of the system, the stable operation of the system will ultimately be affected. For example, when data authenticity is questioned, decision-making processes that depend on such data become unreliable. Compromised data integrity can lead to altered key parameters, such as voltage or current, which undermine the stability of the system. In addition, loss of data privacy exposes sensitive information, leading to economic losses and social challenges. Therefore, it is critical to strengthen security protections at all stages.

Cryptography-based security authentication and privacy preservation methods, centered on identity identification, assign logical identities to devices/users in network communications. These methods authenticate, authorize, and encrypt all access requests, serving as an active defense against cyber attacks. They can effectively safeguard data security and privacy against cyber attacks, gaining widespread attention from scholars both domestically and internationally. In the following, we outline the cryptography-based

security authentication and privacy preservation approaches of CPPSs in Section 3 and Section 4, respectively.

3. Cryptography-Based Security Authentication of CPPSs

Cryptography is a discipline that studies the secure transmission of information, integrating knowledge from mathematics, computer science, and electronic communications, among other fields. In contemporary times, cryptography extends beyond mere data encryption and decryption. It is widely applied for authentication in various scenarios such as industrial internet of things, smart cities, and finance, providing essential information security, including confidentiality, authenticity, integrity, and privacy. In this section, we focus on the authenticity and integrity of data in CPPSs via cryptography-based security authentication. By deeply integrating computing, communication, and control technologies, CPPSs can not only realize the tasks of a single subdomain but also collaborate to complete tasks between multiple subdomains via cross-domain information interaction. A single subdomain refers to an integrated power system that operates in an electrically tightly coupled and fully synchronized manner. In contrast, a multiple subdomain system consists of two or more interconnected subdomains linked via tie-lines. Each subdomain maintains internal frequency synchronization, while power exchange among different regions is typically managed through tie-lines. Due to possible slight frequency deviations among areas, specific control mechanisms are usually required to ensure stable and reliable interconnection. As the cornerstone of information security, cryptography plays a vital role in securing the data interaction of CPPSs. It encompasses secure information exchanges within a single subdomain and across multiple subdomains, providing a solid foundation for the overall security and reliability of CPPSs.

3.1. Security Authentication in a Single Domain of CPPSs

To guarantee secure information interaction in a single CPPS domain, symmetric cryptographic algorithms, such as SM1 [26], SM7 [27], the Data Encryption Standard [28], and the Advanced Encryption Standard [29], have attracted a lot of attention. It uses the same key for encryption and decryption, enabling fast and effective data protection. However, symmetric cryptography is not suitable for large-scale CPPSs due to its low security and high complexity in key distribution and management [30]. Unlike symmetric cryptography, asymmetric cryptography, also known as public-key cryptography, is widely used because of its high security and scalability. It involves a pair of keys (i.e., public and private keys). The two keys are related, but cannot be derived from each other, providing greater flexibility and security for information interaction. In an asymmetric cryptographic algorithm, confidentiality can be safeguarded by encrypting the data using a public key and decrypting the data via a private key; conversely, integrity and authenticity can be ensured by signing the data with a private key and verifying it via a public key. Signature-based [31], key agreement-based [32], and signcryption-based [33] security authentication approaches are studied mainly to protect data security attributes in a single domain of CPPSs.

3.1.1. Signature-Based Security Authentication

Signature-based security authentication methods, as a critical research direction in the field of cryptography, have been widely applied in the network security of CPPSs due to their ability to ensure data integrity and authenticity. Signature-based security authentication can be deployed in distribution domain devices, including smart meters and substation gateways to authenticate electricity consumption data, and ensure the integrity of telemetry messages exchanged with regional distribution control centers. This method enhances the security of the interaction of system information in CPPSs. Recently,

with the continuous advancement of digital signature algorithms and the enhancement of computational capabilities, their role in safeguarding information transmission and system security has become increasingly significant.

To address the issue of secure information interaction of CPPSs, RSA cryptography [34], proposed by Ron Rivest, Adi Shamir, Leonard Adleman, is based on number theory, making it relatively simple to find two large prime numbers but extremely difficult to factor in their product. It has been widely adopted in CPPSs due to its security based on the large integer factorization problem and its simplicity in understanding and implementation [35–37]. The security of RSA relies on the decomposition of large numbers, but research has shown that the 1024-bit key RSA algorithm faces serious security threats. Moreover, the computational speed of RSA is about 1000 times slower than symmetric cryptographic algorithms to achieve the same level of security. Besides the RSA cryptographic algorithm, the digital signature algorithm [38] and the elliptic curve digital signature algorithm [39], which are also designed based on the problem of the difficulty in decomposing large integers, have also been explored and used for CPPS security information interaction.

Compared to RSA, elliptic curve cryptography (ECC), based on the design of the discrete logarithmic hardness problem, independently proposed in 1985 by Neal Koblitz and Victor Miller, provides equivalent security with shorter keys, enhancing computational efficiency while reducing bandwidth and storage requirements under the same security level. It is generally accepted that a 160-bit elliptic curve key provides security strength comparable to a 1024-bit RSA key. Under the same security level, ECC achieves a speed approximately 2.5 times faster than RSA, while asymmetric operations such as key generation and exchange can be 3 to 16 times faster [40]. Considering that, ECC is becoming the mainstream choice for modern cryptographic protocols to design signature schemes for CPPSs [41–45]. The transition from RSA to ECC reflects a significant step toward more efficient and secure cryptography approaches.

With the advent of quantum computing, the emergence of large-scale quantum computers poses a fundamental threat to all classical public-key cryptosystems whose security relies on the hardness of integer factorization or discrete logarithm problems [46]. To address this threat, post-quantum cryptographic schemes, particularly those based on lattice cryptography, are considered to be secure and reliable in the long term [47]. For instance, a linkable ring signature scheme based on NTRU lattice cryptography was constructed under the Raptor framework [48], while a lightweight stateless hash-based signature scheme was designed for resource-constrained industrial IoT devices [49]. The migration from traditional cryptography to post-quantum cryptography is a critical approach to countering future quantum algorithm attacks.

3.1.2. Key Agreement-Based Security Authentication

The signature algorithm ensures the integrity and authenticity of power data, but does not address confidentiality. Key agreement is a method that can safely negotiate shared keys on insecure communication channels and then uses the negotiated keys to encrypt data. For example, secure channels must be established between utility providers and customer-side aggregators before exchanging real-time pricing signals or load adjustment requests. Its fundamental principle allows two communication entities to independently generate the same shared key via public information exchange without pre-shared secrets, simultaneously guaranteeing confidentiality, integrity, and authenticity.

In CPPSs, the open communication environment makes them vulnerable to various cyber threats, including tampering, impersonation, and eavesdropping. They are dedicated to destroying the confidentiality, integrity, and authenticity security aspects. Key agreement mechanisms are essential to ensure reliable power data exchange and system stability.

For example, ElGamal cryptography and the Diffie–Hellman key exchange algorithm were combined to establish a device authentication mechanism, solving the security and cloning problems of authentication and key agreement [50,51]. However, ElGamal-based cryptography involves a large key length and a large number of operations, especially modular exponentiation operations with high computational complexity, resulting in huge computational and communication overheads. These results will inevitably affect system performance, such as state estimation, optimization scheduling, etc. Compared to ElGamal cryptography, ECC reduces key computation, transmission, and storage costs while maintaining a high security level. The key agreement methods of ECC on bilinear pairing [52–57] were presented, which negotiate a session key to achieve secure interaction in CPPSs.

Although bilinear pairing can effectively achieve key agreement for secure information exchange, its multiplication operation time is about 20 times that of elliptic curve scalar multiplication [58]. Thus, it is difficult to apply to power smart terminals, generally embedded devices, with limited computing, communication, and storage resources. Therefore, it is necessary to research ECC-based key agreement without bilinear pairing, reducing computational complexity for resource-constrained smart terminals in CPPSs [59,60]. A method of secure key agreement using pairing-free ECC between local gateways and smart meters [61] and between 5G cellular wireless network devices [62], and a pairing-free ECC authentication key agreement method suitable for smart grids [63,64], were proposed. To improve the practical application of key agreement in advanced metering infrastructure, a protocol of key agreement based on identity and ECC without bilinear pairing was proposed [65]. The above-mentioned references improve the security authentication efficiency for power smart terminals. Despite the aforementioned advances, the security of classical cryptography-based key agreement protocols similarly faces threats from quantum adversaries. Lattice-based key agreement schemes have been introduced as quantum-safe alternatives. Kim et al. [66] proposed a hybrid authentication and key exchange protocol based on ML-KEM. Bagchi et al. [67] designed a quantum-safe three-party authenticated key agreement protocol based on ring learning with errors cryptography, offering resistance against quantum attacks.

Nevertheless, no matter how efficient the key agreement method is for identity authentication, if a key is compromised, all operations related to that key become insecure. However, the previous literature does not consider the security risks posed by key leakage of power devices. To address this, revocable multiauthentication key agreement methods [68,69] were designed, employing a fixed key update strategy. However, if a key is leaked during the update cycle, it may result in untimely key updates, making transmitted information insecure. The dynamic key update strategy was used to renew the keys of compromised devices, forming new approaches to key agreement [70,71]. This enhances the security of the interaction of system information in CPPSs.

3.1.3. Signcryption-Based Security Authentication

Key agreement needs to establish the session key via a signature algorithm, and further encrypt data with the session key to ensure data confidentiality. This method, which first verifies the identity of the device through signing and then uses a negotiated session key for data encryption, undoubtedly increases computational costs and the number of communications.

The signcryption method successfully addresses the aforementioned issue, improving the coupling of encryption and digital signature functions. Signcryption-based authentication can realize both encryption and signature functions in a single operational step, while simultaneously ensuring confidentiality, authenticity, and integrity of transmitted

information [72]. Under the same communication security objectives, signcryption-based authentication significantly reduces computation and communication overheads, improving overall authentication efficiency [73]. It enhances the efficiency of identity security authentication between devices, thereby reducing the latency caused by security authentication in CPPSs [74]. It involves encryption and signature, enabling to simultaneously realize confidentiality, authenticity, and integrity. Signcryption has been widely applied in practical CPPS information security authentication scenarios due to its advantages. For example, in wide-area monitoring systems, phasor measurement units must transmit time-synchronized measurements with both confidentiality and authenticity. Signcryption schemes based on identity-based cryptography (IBC) were presented for smart grids, ensuring secure data access [75–77]. To adapt to more complex and varied application scenarios and further improve security, efficiency, and flexibility, generalized signcryption methods based on IBC [78,79] were developed to ensure secure information exchange between power devices. Considering a large number of devices, a signcryption method based on IBC and blockchain was proposed, which can authorize multiple recipients simultaneously [80]. These methods focus on identity authentication through a single cryptography. In the increasingly complex network environment of CPPSs, different service systems always adopt their preferred cryptography protocols, leading to potential interoperability barriers in information exchange. To ensure that these heterogeneous systems can seamlessly and securely share data, a heterogeneous signcryption method based on public key infrastructure and IBC has been proposed [81,82], supporting the interaction of secure power data between different cryptographic systems of CPPSs.

IBC is widely studied, but its key escrow issue (i.e., overreliance on third parties) can cause insecure keys [83]. To address this inherent problem of IBC while retaining its advantages of not needing key certificates, a certificateless cryptography (CLC) method has emerged. The main idea is that the key generation center (that is, the key generator for the power entities of the CPPSs) collaborates with the device to construct the keys [84,85]. CLC-based signcryption approaches were investigated, allowing authorized devices to ensure confidentiality, integrity, and authenticity [86–88]. According to CLC, generalized signcryption protocols have been proposed to improve authentication security and efficiency [89,90]. Furthermore, hybrid signcryption based on public key infrastructure and CLC [91] and heterogeneous hybrid signcryption based on IBC and CLC [92] were introduced, addressing secure communication in heterogeneous cryptosystems of CPPSs. To address the threat of quantum attacks, certificateless signcryption schemes based on lattice cryptography have also been proposed [93].

Tables 3 and 4 summarize the security authentication methods based on signature, key agreement, and signcryption approaches in a single CPPS domain. Table 3 presents the cryptographic primitives and their supported security attributes, namely confidentiality, integrity, and authenticity, while Table 4 provides quantitative performance comparisons in terms of key length and signature size under an equivalent security level (e.g., 128-bits security level). Under the same security level, RSA suffers from low efficiency due to the high overhead of key generation and signature. In contrast, ECC achieves high efficiency because of its compact keys and signatures and fast computation. ML-DSA-44 offers fast computation, but its key and signature sizes are much larger than those of the previous two, placing its efficiency at medium.

Table 3. Comparisons between signature-based, key agreement-based, signcryption, and post-quantum signature-based security authentication in a single domain of CPPSs.

Security Authentication Method	Cryptography Algorithm	Confidentiality./Integrity./Authenticity.
Signature-based	RSA [35–37]	X/✓/✓
	Digital signature algorithm [38]	
	Elliptic curve digital signature algorithm [39]	
	ECC [41–45]	
	Lattice-based Cryptography [48]	
	Hash-based Cryptography [49]	
Key agreement-based	ElGamal [50,51]	X/✓/✓
	ECC on bilinear pairing [52–57]	
	ECC without bilinear pairing [59–65]	
	Lattice-based Cryptography [66,67]	
Signcryption-based	IBC [75–79]	✓/✓/✓
	Public key infrastructure and IBC [81,82]	
	CLC [86–90]	
	Public key infrastructure and CLC [91]	
	IBC and CLC [92]	
	Lattice-based Cryptography [93]	

Table 4. Comparison of features and efficiency of classic cryptographic methods.

Cryptographic Method	Public Key Size	Signature Size	Efficiency Under Same Security Level and Security Property
RSA	3072 bits	3072 bits	Low
ECC	520 bits	512 bits	High
ML-DSA-44 (Lattice-based)	10,496 bits	19,360 bits	Medium

3.2. Cross-Domain Security Authentication Among Multiple Domains of CPPSs

CPPSs are often divided into different subdomains due to their large scale, which requires frequent data exchange to collaborate to accomplish the same tasks, as shown in Figure 3. To ensure the security of CPPSs, cross-domain security authentication to verify identity among multiple domains of power devices in CPPSs is essential.

Driven by the advantages of blockchain-based security mechanisms of decentralization, anonymity, complete transparency, and high security, it has expanded from the realm of virtual currencies to other fields, such as CPPSs [94,95]. In peer-to-peer energy trading among distributed energy resources, blockchain can provide immutable transaction ledgers and automated settlement via smart contracts, reducing reliance on centralized market operators. Additionally, in the coordination of virtual power plants and multi-microgrids, blockchain facilitates secure and auditable data exchange among heterogeneous participants. The emergence of blockchain technology provides relevant solutions to enable secure information interaction across multiple subdomains to facilitate collaboration. Cross-domain security authentication mechanisms based on alliance blockchain were investigated, achieving identity authentication among different configured subdomains in CPPSs [96–98]. A cross-domain authentication method was proposed based on a multi-certificate authentication system and blockchain, which establishes distributed trust to achieve interdomain

authentication [99]. In order to address the information security and privacy issues that arise from the integration of distributed energy into traditional power grids, a framework based on blockchain and a software-defined network was proposed, which ensures the security of energy transactions and data communications [100].

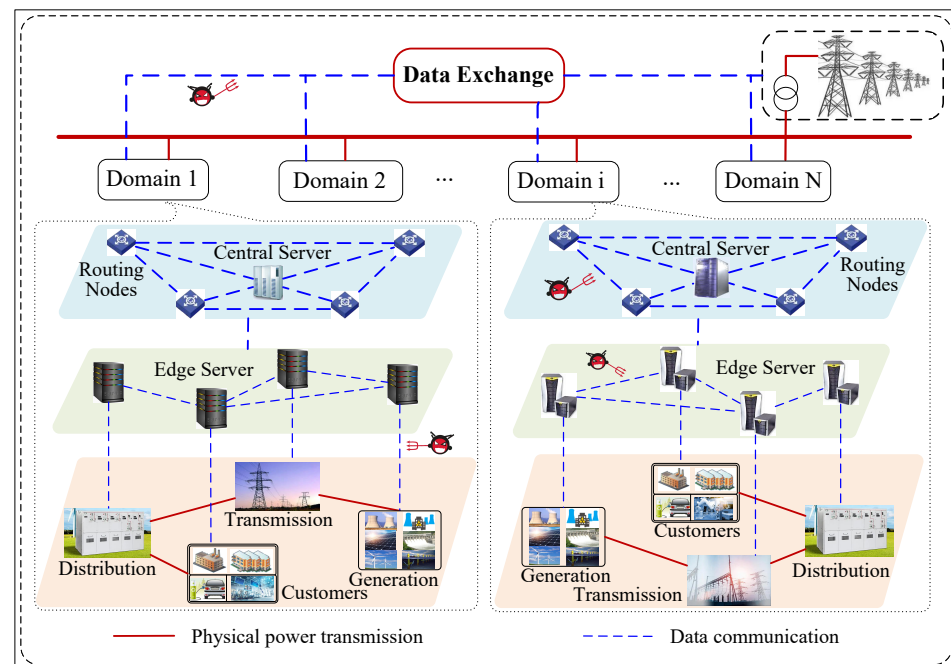


Figure 3. Data exchange in A CPPS scenario with multiple domains.

The aforementioned literature employs a single blockchain for cross-domain authentication of interdomain power devices. Given that a single blockchain must store a vast amount of information on power equipment, this approach imposes a significant storage burden, leading to low certification efficiency in CPPSs. To address this challenge, the concept of dual chain collaboration has emerged for the exchange of data security among domains [101,102]. References [103,104] explored cross-domain authentication schemes with dual blockchains featuring bilinear pairing. Although these approaches improve the system's certification efficiency, the inherent transparency of blockchains means that they cannot ensure the confidentiality of the data being exchanged. As a result, attackers can easily obtain original power operation and control data, which may compromise the stable operation of CPPSs. The signcryption algorithm provides the confidentiality, integrity, and authenticity of data simultaneously. The combination of blockchain and signcryption algorithm can solve the above problem and allows more security aspects for CPPSs [105].

Beyond security authentication that ensures secure information exchange, CPPSs contains a large amount of sensitive data (e.g., customer privacy and electricity behavior data, grid topology and critical facility data, and market transactions and commercially sensitive data). The preservation of data privacy in CPPSs is also extremely significant. Therefore, in Section 4, we outline the privacy-preserving methods based on cryptography of CPPSs.

4. Cryptography-Based Privacy Preservation of CPPSs

With the continuous development and refinement of CPPSs, the demand for the preservation of data privacy has become increasingly prominent [106]. In particular, as cloud computing becomes deeply integrated with CPPSs, sensitive power information originally stored locally has been widely deployed in the cloud, exposing higher risks of data leakage [107]. Therefore, research on effective privacy preservation methods to ensure the

security of power data has become a critical issue to be addressed in the CPPS cloudification process.

To achieve the goal of protecting the privacy of CPPSs, secure multiparty computation [108–111], federal learning [112–114], a trusted computing platform [115,116], data desensitization [117,118], differential privacy [119–121], and homomorphic encryption methods are researched. These approaches can be divided into four types from the data flow and data computation perspectives, which are summarized in Figure 4. From the perspective of data flow, two situations occur with respect to the preservation of privacy. In the first situation, the data will flow out of the local area, where the data are available but not visible; another situation is that the data do not flow out, where the data do not move but the program moves. From the point of view of data computation, centralized and collaborative computing are divided. It clearly shows that secure multiparty computation belongs to collaborative computation and data flow. Secure multiparty computation allows multiple data owners to perform collaborative computations without mutual trust, producing computation results while ensuring that the data remain usable but invisible. Federated learning does not require data to flow out and is computed collaboratively by the participating parties. It distributes machine learning algorithms to parties that possess data, and then every party transmits the training parameters back. Relying on centralized computing without flowing out the data, trusted computing platform constructs a secure and controllable area via hardware-level isolation mechanisms, guaranteeing the privacy and integrity of the internal data. Data desensitization, differential privacy, and homomorphic encryption use centralized computation and available but not visible data to protect privacy.

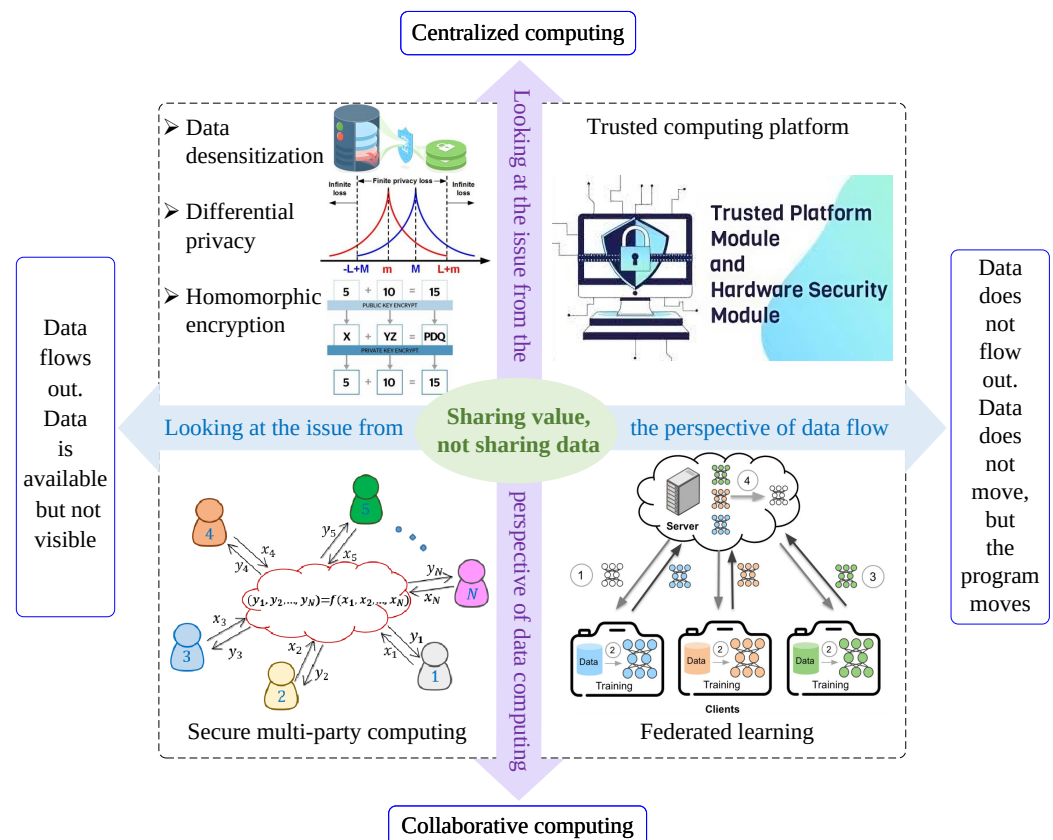


Figure 4. Different privacy-preserving methods. M and m are the central privacy loss of two distributions for neighboring datasets, L denotes global sensitivity. X , Y , and PDQ stand for ciphertexts generated via homomorphic encryption of plaintext data.

Among these methods, none of data desensitization, differential privacy, trusted computing platform, and federal learning can directly perform computations or analyzes on encrypted data. This means that untrustworthy third parties (e.g., cloud servers) can decrypt and access the original power data, failing to guarantee privacy during the data computation process. Secure multiparty computation can effectively solve this problem by allowing multiple participants to collaboratively calculate an agreed-upon function, while ensuring that each participant can only obtain its own computation results. That is, secure multiparty computation effectively protects data privacy as each participant cannot infer the input or output data of any party from the interaction data during the computation. However, its efficiency is relatively low because of the need for multi-party collaborative computation. Despite its computation overhead, SMPC is well-suited for large-timescale tasks that can tolerate latency. In power flow analysis scenarios, SMPC enables multiple parties to jointly perform computations without revealing their respective private inputs [122]. Meanwhile, federated learning integrated with SMPC and differential privacy techniques ensures data privacy protection while maintaining prediction accuracy, facilitating short-term load and renewable generation forecasting in smart grids [123].

Homomorphic encryption preserves data privacy from a cryptographic viewpoint, which is more suitable for one-sided outsourced calculations, but usually with complex computation [124]. The core value of homomorphic encryption is realized through end-to-end ciphertext computation throughout the entire process. For example, calculating total regional load from encrypted meter readings, or executing economic dispatch algorithms without decrypting individual generator bids. Here, we mainly focus on investigating the homomorphic encryption-based privacy preservation method, protecting the data privacy security of CPPSs during the collection, transmission, and computation processes. Homomorphic encryption is a special encryption technique that allows computation to be performed on encrypted data, preventing data privacy leakage during the communication, storage, and computation processes of various applications. Depending on the types and complexity of the supporting operation, homomorphic encryption can be categorized into partially homomorphic encryption, somewhat homomorphic encryption, and fully homomorphic encryption.

Partially homomorphic encryption is researched to protect the privacy of CPPSs. For example, an ElGamal-based [125] and an elliptic curve ElGamal-based homomorphic encryption algorithm were proposed to protect the privacy of real-time electricity consumption data through homomorphic addition operations [126]. Moreover, Paillier cryptography-based homomorphic encryption algorithms were designed to perform addition computation on encrypted power data to achieve privacy preservation [127–131]. An edge-assisted mobile crowd sensing method based on bilinear pairing and homomorphic encryption was proposed to protect privacy via homomorphic multiplication operations [132]. However, the partially homomorphic encryption supports only one specific type of mathematical operation (either addition or multiplication), although the number of operations is not limited.

To support multiple types of operation, somewhat homomorphic encryption is studied to allow for a limited number of addition and multiplication operations on ciphertext. A privacy preservation method using bilinear pairing was investigated in relation to smart grids, which can execute homomorphic addition and multiplication operations [133]. An encrypted data sharing scheme based on the Boneh–Goh–Nissim cryptosystem was researched, which executes a one-time multiplication and infinite additions on ciphertext [134]. A somewhat homomorphic encryption cryptosystem based on the confused modulo projection theorem was studied, allowing the server to complete blind data processing without seeing the effective information of the user data [135]. Apart from data privacy,

somewhat homomorphic encryption is used to protect image information privacy [136]. Somewhat homomorphic encryption has already demonstrated its significant potential in specific scenarios, capable of supporting a limited number of homomorphic addition and multiplication operations. However, the limitation of somewhat homomorphic encryption lies in its ability to handle only circuits of limited depth, which restricts its application in complex computational tasks, such as optimizing and predicting of CPPSs.

To overcome the above limitation, fully homomorphic encryption is developed to protect data privacy. It can support computations of arbitrary depth, meaning that arbitrarily complex calculations can be performed on encrypted data without decrypting intermediate results. Gentry proposed the first fully homomorphic encryption scheme based on an ideal lattice, which eliminates noise by bootstrapping [137]. It allows an arbitrary number of addition and multiplication operations and resists quantum attacks. Since then, homomorphic encryption has triggered significant interest, and novel constructions of fully homomorphic encryption have been proposed following Gentry's idea, including Brakerski–Gentry–Vaikuntanathan [138], Fan–Vercauteren [139], Cheon–Kim–Kim–Song [140] and torus fully homomorphic encryption [141]. These representatives rely on the hard problems of learning with errors or ring learning with errors with the advantages of high security, low computation complexity, and strong adaptability. For example, a Brakerski–Gentry–Vaikuntanathan-based fully homomorphic encryption algorithm was proposed to protect sensitive user data in smart grids [142]. A multiidentity fully homomorphic encryption scheme based on learning with errors was presented for edge-enabled smart grids, which ensures the computation security in edge nodes [143].

5. Challenge Issues

This article addresses the challenge of insecure information interaction and privacy leakage in CPPSs under cyber attacks. From the perspective of active defense, we review cryptography-based security authentication and privacy-preservation methods. However, several unsolved challenges remain in this area, which are summarized below.

5.1. The Intersection of Cryptography and Networked Control for CPPSs

As CPPSs evolve toward intelligence and distribution, the in-depth integration of networked control and cryptography has become critical to ensuring system security. Post-quantum cryptography [144], as a core technology for resisting quantum computing attacks, will reconstruct the security control paradigm of power systems when combined with control theory. This direction faces multiple challenges in the future.

There is an inherent contradiction between the high computational complexity of post-quantum cryptographic algorithms and the real-time requirements of power control [145]. Encryption of control signals must be deeply coupled with control algorithms. In distributed cooperative control, for example, encryption operations may alter the temporal characteristics of control signals, increasing bandwidth usage and affecting the dynamic response speed of algorithms such as load frequency control. This necessitates collaborative optimization through lightweight design of encryption protocols and adaptive adjustment of control parameters.

5.2. Scalability of Blockchain in CPPSs

Although blockchain-based security mechanisms can ensure secure information interaction among multiple subregions in CPPSs, the introduction of diverse entities (e.g., energy aggregators and integrated energy service providers) and new services (e.g., virtual power plants and electric vehicles) diversifies interaction patterns, resulting in new characteristics of data exchange such as large volume and frequent interactions. Traditional blockchain

technology faces severe network congestion when transaction data volume increases significantly, leading to high delays in power data authentication processes. Therefore, it is crucial to investigate how to achieve blockchain scalability, which refers to the ability of the blockchain network to expand efficiently when handling more transaction data. To achieve this high performance, sharding [146] and consensus mechanism optimization [147] techniques can be adopted, guaranteeing the scalability of blockchain. Enhancing blockchain scalability will enable the network to process larger volumes of transaction data while maintaining high performance and better satisfying the real-time requirements of CPPSs.

5.3. Convergence of Cryptography and Artificial Intelligence

Combining cryptography, the cornerstone of information security, with increasingly evolving artificial intelligence (AI) technologies can provide powerful data protection capabilities. Cryptography has evolved from the AI-unaware cryptography stage, where it was vulnerable to AI attacks, to the AI-embedded cryptography stage, where AI techniques are applied to basic encryption and decryption components, and finally to the development of the fusion of the two. For example, a neural network learning method is exploited to accelerate core data processing procedures in quantum key distribution systems [148], while a reinforcement learning framework is adopted to realize intelligent dynamic matching of quantum-safe cryptographic schemes for resource-limited terminal environments [149]. Despite these benefits, AI-embedded cryptography in CPPSs faces concrete risks from adversarial machine learning. Attackers can craft imperceptible perturbations to power data, misleading AI-based cryptanalysis or key management systems and potentially compromising encryption and authentication processes. Such threats are particularly critical in CPPSs, where compromised cryptographic operations could propagate into the physical domain and affect control decisions. ‘In the future, “quantum AI-enabled cryptography” may become an important development direction to further optimize the performance of AI decision-making and machine learning algorithms for more complex problems, especially with further research in the fields of quantum-inspired neural networks and quantum-inspired reinforcement learning. In addition, AI technology will also play a key role in the development of post-quantum cryptographic algorithms; for example, deep learning, machine learning, generative AI, and other technologies will provide technical support in strengthening the ability of cryptographic systems to cope with attacks by quantum computers, and further enhance the ability of the field of cryptography to cope with rapid changes in technology.

6. Conclusions

With the rapid development of the smart grid, CPPSs face increasingly complex security threats and privacy preservation challenges while providing intelligent power management. In this paper, we systematically review the application of cryptography in CPPS security authentication and privacy preservation, and analyze the cyber attacks (e.g., false data injection attack, data replay attack, and man-in-the-middle attack) in CPPSs, as well as the scenarios in which generation, transmission, distribution, and consumption are susceptible to cyber attacks. We not only review the information security authentication within a single subdomain, but also include information cross-domain security authentication among multiple subdomains. In addition to information security authentication, this paper also summarizes cryptography-based privacy-preserving methods and presents the applicability and limitations of different cryptographic schemes in the smart grid environment. Three future research directions are also highlighted for information security interaction in CPPSs to promote potential interest in this research direction.

Author Contributions: Methodology, C.J.; Investigation, C.J. and H.Y.; Validation, C.J. and L.W.; Supervision, C.J., H.Y., and M.W.; Writing—review and editing, C.J., L.W. and R.F.; Software, J.B.; Writing—original draft, J.B.; Project administration, H.Y. and M.W.; All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Joint Funds of the National Natural Science Foundation of China under Grant No. U23B2021, and the Shanghai Pujiang Program of China under Grant No. 25PJD047.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors would like to thank the anonymous reviewers for their constructive comments.

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

Abbreviations

The following abbreviations are used in this manuscript:

CPPS	cyber-physical power system
ECC	elliptic curve cryptography
IBC	identity-based cryptography
CLC	certificateless cryptography
SMPC	secure multiparty computation
AI	artificial intelligence

References

1. Cai, Y.; Zhan, W.; Shi, X.; Tang, L.; Tang, X.; Cao, Y. Reliability analysis of power cyber-physical systems based on cross-domain fault interface matrices. *Sustain. Energy Grids Netw.* **2025**, *44*, 102058.
2. Li, J.; Wang, Y.; Li, H.; Wang, H.; Su, Q. Adaptive dual control law sliding mode observer to reconstruct cyber attack and compensate power in cyber physical power system. *IEEE Trans. Power Syst.* **2025**, *40*, 3198–3210.
3. Li, X.; Xu, Q.; Lu, X.; Lin, M.; Chen, C.; Guan, X. Distributionally robust coordinated defense strategy for time-sensitive networking enabled cyber–physical power system. *IEEE Trans. Smart Grid* **2024**, *15*, 3278–3287.
4. Bhattacharjee, A.; Bai, G.; Tushar, W.; Verma, A.; Mishra, S.; Saha, T.K. DeeBBAA: A benchmark deep black-box adversarial attack against cyber–physical power systems. *IEEE Internet Things J.* **2024**, *11*, 40670–40688.
5. Sureshkumar, V.; Anandhi, S.; Amin, R.; Selvarajan, N.; Madhumathi, R. Design of robust mutual authentication and key establishment security protocol for cloud-enabled smart grid communication. *IEEE Syst. J.* **2021**, *15*, 3565–3572.
6. Qin, C.; Hu, X.; Zhong, C.; Zeng, Y. Vulnerability analysis of power system under uncertain cyber-physical attacks based on stochastic bi-level optimization. *Sustain. Energy Grids Netw.* **2025**, *42*, 101647.
7. Tooki, O.O.; Popoola, O.M. A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems. *Renew. Energy Focus* **2024**, *51*, 100628.
8. Feng, Y.; Huang, R.; Zhao, W.; Yin, P.; Li, Y. A survey on coordinated attacks against cyber-physical power systems: Attack, detection, and defense methods. *Electr. Power Syst. Res.* **2025**, *241*, 111286.
9. Kabir, S.; Hannan, N.; Shufian, A.; Zishan, M.S.R. Proactive detection of cyber-physical grid attacks: A pre-attack phase identification and analysis using anomaly-based machine learning models. *Array* **2025**, *27*, 100441.
10. Li, X.; Li, B.; Li, H. Intelligent detection and early warning of power system cybersecurity threats based on multi-modal large language models. *J. Cyber Secur. Mobil.* **2025**, *14*, 1375–1400.
11. Wu, Y.; Guo, H.; Han, Y.; Li, S.; Liu, J. A security-enhanced authentication and key agreement protocol in smart grid. *IEEE Trans. Ind. Inform.* **2024**, *20*, 11449–11457.
12. Abdalzaher, M.S.; Fouda, M.M.; Emran, A.; Fadlullah, Z.M.; Ibrahim, M.I. A survey on key management and authentication approaches in smart metering systems. *Energies* **2023**, *16*, 2355.

13. Mall, P.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.-K.R. PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: A comprehensive survey. *IEEE Internet Things J.* **2022**, *9*, 8205–8228.
14. Mishra, N.; Islam, S.K.H.; Zeadally, S. A survey on security and cryptographic perspective of Industrial-Internet-of-Things. *Internet Things* **2024**, *25*, 101037.
15. Hassan, M.U.; Rehmani, M.H.; Chen, J. Differential privacy techniques for cyber physical systems: A survey. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 746–789.
16. Husnoo, M.A.; Anwar, A.; Chakraborty, R.K.; Doss, R.; Ryan, M.J. Differential privacy for IoT-enabled critical infrastructure: A comprehensive Survey. *IEEE Access* **2021**, *9*, 153276–153304.
17. Li, Y.; Cao, L.; Zheng, G.; Men, H.; Chen, L. Improved RSA dynamic cryptographic accumulator-based anonymous batch authentication scheme for internet of vehicles. *Comput. Electr. Eng.* **2024**, *117*, 109261.
18. Naderi, E.; Asrari, A. A deep learning framework to identify remedial action schemes against false data injection cyberattacks targeting smart power systems. *IEEE Trans. Ind. Inform.* **2024**, *20*, 1208–1219.
19. Shen, K.; Yan, W.; Ni, H.; Chu, J. Localization of false data injection attack in smart grids based on SSA-CNN. *Information* **2023**, *14*, 180.
20. Kumar, K.; Kumar, P.; Kar, S. A blockchain-enabled framework for secure synchronization and resilient energy distribution in networked microgrids against false data attacks. *Sustain. Energy Grids Netw.* **2025**, *44*, 101880.
21. Ramanan, P.; Li, D.; Gebrael, N. Blockchain-based decentralized replay attack detection for large-scale power systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *52*, 4727–4739.
22. De, S.; Sodhi, R. A replay-attack-resilient power system state estimation scheme. *IEEE Trans. Autom. Sci. Eng.* **2025**, *22*, 13588–13602.
23. Jena, S.; Padhy, N.P.; Guerrero, J.M. Multi-layered coordinated countermeasures for DC microgrid clusters under man in the middle attack. *IEEE Trans. Ind. Appl.* **2024**, *60*, 2127–2141.
24. Du, D.; Zhu, M.; Li, X.; Fei, M.; Bu, S.; Wu, L.; Li, K. A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems. *J. Mod. Power Syst. Clean Energy* **2023**, *11*, 727–743.
25. Li, X.; Yang, J.; Du, D.; Zhou, Z.; Li, K.; Wu, L. Resilient distributed economic dispatch for cyber-physical power systems considering carbon emissions trading and false data injection attacks. *Energy* **2025**, *332*, 136881. <https://doi.org/10.1016/j.energy.2025.136881>.
26. Xuhui, Z.; Na, L.; Peihua, K.; Boyang, L. Design of the networked electric meter based on GPRS. In Proceedings of the 4th International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), Harbin, China, 18–20 September 2014; pp. 230–234.
27. Guo, Z.; Li, N.; Li, Y.; Rui, G. SM7 authentication key distribution algorithm for power field operation intelligent terminal. In Proceedings of the International Conference on Wireless Communications and Smart Grid (ICWCSG), Hangzhou, China, 13–15 August 2021; pp. 209–212.
28. Cui, A.; Zhao, H.; Zhang, X.; Zhao, B.; Li, Z. Power system real time data encryption system based on DES algorithm. In Proceedings of the 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Beihai, China, 16–17 January 2021; pp. 220–228.
29. Iqbal, A.; Iqbal, T. Low-cost and secure communication system for remote micro-grids using AES cryptography on ESP32 with lora module. In Proceedings of the IEEE Electrical Power and Energy Conference (EPEC), Toronto, ON, Canada, 10–11 October 2018; pp. 1–5.
30. Zhang, J.; Zhang, F.; Huang, X. Theory and applications of sequentially threshold public-key cryptography: Practical private key safeguarding and secure use for individual users. *IEEE Trans. Inf. Forensics Secur.* **2025**, *20*, 3220–3233.
31. Meshram, C.; Obaidat, M.S.; Tembhurne, J.V.; Shende, S.W.; Kalare, K.W.; Meshram, S.G. A lightweight provably secure digital short-signature technique using extended chaotic maps for human-centered IoT systems. *IEEE Syst. J.* **2021**, *15*, 5507–5515.
32. Hu, S.; Chen, Y.; Zheng, Y.; Xing, B.; Li, Y.; Zhang, L.; Chen, L. Provably secure ecc-based authentication and key agreement scheme for advanced metering infrastructure in the smart grid. *IEEE Trans. Ind. Inform.* **2023**, *19*, 5985–5994.
33. Li, X.; Jiang, C.; Du, D.; Zhou, Z.; Fei, M.; Wu, L. Cyber-physical power systems: Exploring a streamlined signcryption scheme for resource-limited smart terminals. *IEEE Trans. Ind. Inform.* **2024**, *20*, 9749–9760.
34. Bao, Z.; He, D.; Feng, Q.; Luo, M.; Zeng, X. Constant-size verifiable timed signatures from rsa group for bitcoin-based voting protocols. *IEEE Trans. Serv. Comput.* **2024**, *17*, 1414–1425.
35. Avestro, J.E.; Sison, A.M.; Medina, R.P. Hybrid algorithm combining modified Diffie Hellman and RSA. In Proceedings of the 4th International Conference on Technology, Informatics, Management, Engineering & Environment (TIME-E), Bali, Indonesia, 13–15 November 2019; pp. 100–104.
36. Kong, W.; Shen, J.; Vijayakumar, P.; Cho, Y.; Chang, V. A practical group blind signature scheme for privacy protection in smart grid. *J. Parallel Distrib. Comput.* **2020**, *136*, 29–39.

37. Qian, J.; Cao, Z.; Lu, M.; Chen, X.; Shen, J.; Liu, J. The secure lattice-based data aggregation scheme in residential networks for smart grid. *IEEE Internet Things J.* **2022**, *9*, 2153–2164.
38. Sharma, M.K.; G, K.; Kumari, A. Studying the performance of digital signature algorithms in information security models for networking applications. In Proceedings of the 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA), Namakkal, India, 15–16 March 2024; pp. 1–6.
39. Zhang, H.; Liu, X.; Li, B. FPGA implementation of elliptic curve digital signature algorithm based on PUFs. In Proceedings of the 9th International Conference on Signal and Image Processing (ICSIP), Nanjing, China, 12–14 July 2024; pp. 520–525.
40. Vardhan, K.L.H.; Jain, V. Enhanced secure file transfer: A comparative analysis of elliptic curve cryptography vs. RSA. In Proceedings of the 2025 International Conference on Advanced Computing Technologies (ICoACT), Sivakasi, India, 14–15 March 2025; pp. 1–6.
41. Shukla, S.; Thakur, S.; Breslin, J.G. Secure communication in smart meters using elliptic curve cryptography and digital signature algorithm. In Proceedings of the IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021; pp. 261–266.
42. Li, W.; Li, R.; Wu, K.; Cheng, R.; Su, L.; Cui, W. Design and implementation of an SM2-based security authentication scheme with the key agreement for smart grid communications. *IEEE Access* **2018**, *6*, 71194–71207.
43. Aitzhan, N.Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 840–852.
44. Chaudhry, S.A.; Yahya, K.; Garg, S.; Kaddoum, G.; Hassan, M.M.; Zikria, Y.B. LAS-SG: An elliptic curve-based lightweight authentication scheme for smart grid environments. *IEEE Trans. Ind. Inform.* **2023**, *19*, 1504–1511.
45. Wang, W.; Xu, H.; Alazab, M.; Gadekallu, T.R.; Han, Z.; Su, C. Blockchain-based reliable and efficient certificateless signature for IIoT devices. *IEEE Trans. Ind. Inform.* **2022**, *18*, 7059–7067.
46. Bhoi, S.S.; Saini, A.; Diro, A.; Kaisar, S.; Rao, A. Future digital identity management with quantum secure blockchain. *IEEE Commun. Surv. Tutor.* **2026**, *28*, 1679–1708.
47. Oonishi, K.; Kunihiro, N. Shor’s algorithm using efficient approximate quantum Fourier transform. *IEEE Trans. Quantum Eng.* **2023**, *4*, 1–16.
48. Kuninets, A.; Malygina, E.; Nesterenko, A. On a lattice-based post-quantum ring signature scheme. *J. Comput. Virol. Hacking Tech.* **2026**, *22*, 15.
49. Liu, C.-H. Lightweight hash-based post-quantum signature scheme for industrial Internet of Things. *Comput. Mater. Contin.* **2025**, *86*, 1–18.
50. Prasad, M.; Manoharan, R. DS-AKA-A novel secured authentication protocol for LTE-A using public key cryptography. *J. Internet Technol.* **2017**, *18*, 753–763.
51. Vatchala, S.; Ravimaran, S.; Sathish, A. Auto sec SDN-XTR: A hybrid end to end security mechanism with efficient trace representation on open stack cloud. *J. Inf. Sci. Eng.* **2019**, *35*, 697–718.
52. Tsai, J.; Lo, N. Secure anonymous key distribution scheme for smart grid. *IEEE Trans. Smart Grid* **2016**, *7*, 906–914.
53. Odelu, V.; Das, A.K.; Wazid, M.; Conti, M. Provably secure authenticated key agreement scheme for smart grid. *IEEE Trans. Smart Grid* **2018**, *9*, 1900–1910.
54. Nyangaresi, V.O.; Ghaib, A.A.; Jasim, H.M.; Abduljabbar, Z.A.; Ma, J.; Al Sibaehe, M.A.; Aldarwish, A.J.Y.; Ali, A.H.; Neamah, H.A. Message verification protocol based on bilinear pairings and elliptic curves for enhanced security in vehicular Ad Hoc networks. *CMC-Comput. Mater. Contin.* **2024**, *8*, 1029–1057.
55. Farooq, S.M.; Hussain, S.M.S.; Ustun, T.S.; Iqbal, A. Using ID-based authentication and key agreement mechanism for securing communication in advanced metering infrastructure. *IEEE Access* **2020**, *8*, 210503–210512.
56. Zhang, T.; Lu, X.; Ji, X.; Xu, W. An identity-based secure communication scheme for advanced metering infrastructure in smart grid. In Proceedings of the 29th Chinese Control and Decision Conference (CCDC), Chongqing, China, 28–30 May 2017; pp. 6959–6964.
57. Chen, Y.; Martínez, J.-F.; Castillejo, P.; López, L. A bilinear map pairing based authentication scheme for smart grid communications: PAuth. *IEEE Access* **2019**, *7*, 22633–22643.
58. Ali, I.; Chen, Y.; Ullah, N.; Kumar, R.; He, W. An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1278–1291.
59. Ma, H.; Wang, C.; Xu, G.; Cao, Q.; Xu, G.; Duan, L. Anonymous authentication protocol based on physical unclonable function and elliptic curve cryptography for smart grid. *IEEE Syst. J.* **2023**, *17*, 6425–6436.
60. Li, X.; Jiang, C.; Du, D.; Fei, M.; Wu, L. A novel revocable lightweight authentication scheme for resource-constrained devices in cyber-physical power systems. *IEEE Internet Things J.* **2023**, *10*, 5280–5292.
61. Srinivas, J.; Das, A.K.; Li, X.; Khan, M.K.; Jo, M. Designing anonymous signature-based authenticated key exchange scheme for internet of things-enabled smart grid systems. *IEEE Trans. Ind. Inform.* **2021**, *17*, 4425–4436.

62. Kabi, M.; Dayal, N.; Raikwal, P. ECC-based lightweight authentication for resource-constrained devices leveraging the edge node. *IEEE Trans. Reliab.* **2025**, *74*, 2605–2612.
63. Khan, A.A.; Kumar, V.; Prasad, R.; Idrisi, M.J. SGAK: A robust ecc-based authenticated key exchange protocol for smart grid networks. *IEEE Access* **2024**, *12*, 195745–195759.
64. Qi, M.; Chen, J. Two-pass privacy preserving authenticated key agreement scheme for smart grid. *IEEE Syst. J.* **2021**, *15*, 3201–3207.
65. Mohammadali, A.; Sayad Haghighi, M.; Tadayon, M.H.; Mohammadi-Nodooshan, A. A novel identity-based key establishment method for advanced metering infrastructure in smart grid. *IEEE Trans. Smart Grid* **2018**, *9*, 2834–2842.
66. Kim, J.; Woo, N.; Ryu, J. A post-quantum resistant lightweight key authentication and exchange protocol for smart home environments. *IEEE Access* **2026**, *14*, 59439–59453.
67. Bagchi, P.; Roy, A.; Wazid, M.; Das, A.K.; Bhargava, B.K.; Park, Y. Big data analytics-envisioned quantum-safe lattice-based three-party authenticated key agreement protocol for cloud IoT-enabled healthcare applications. *IEEE Trans. Dependable Secur. Comput.* **2026**, *23*, 368–385.
68. Li, W.; Li, X.; Gao, J.; Wang, H. Design of secure authenticated key management protocol for cloud computing environments. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 1276–1290.
69. Lee, K. Comments on “Secure data sharing in cloud computing using revocable-storage identity-based encryption”. *IEEE Trans. Cloud Comput.* **2020**, *8*, 1299–1300.
70. Shim, K.-A. Comments on “revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks”. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 81–82.
71. Hsu, R.-H.; Lee, J.; Quek, T.Q.S.; Chen, J.-C. GRAAD: Group anonymous and accountable D2D communication in mobile networks. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 449–464.
72. Shaw, S.; Dutta, R. A quantum resistant multi-user signcryption scheme featuring key invisibility for Internet of Things. *J. Inf. Secur. Appl.* **2023**, *76*, 103549.
73. Dai, C.; Xu, Z. Pairing-free certificateless aggregate signcryption scheme for vehicular sensor networks. *IEEE Internet Things J.* **2023**, *10*, 5063–5072.
74. Han, Y.; Zhou, Y.; Yang, B.; Xia, Z.; Zhang, M. An efficient and secure lightweight certificateless hybrid signcryption scheme. *IEEE Internet Things J.* **2024**, *11*, 12252–12265.
75. Patil, R.; Patil, Y.H. A secure and efficient identity-based proxy signcryption scheme for smart grid network. *J. Eng. Sci. Technol. Rev.* **2022**, *15*, 82–89.
76. Li, S. A new signcryption algorithm for secure communication in Ad Hoc networks. *Int. J. Auton. Adapt. Commun. Syst.* **2021**, *14*, 196–212.
77. Ye, F.; Qian, Y.; Hu, Q.Y. Identity-based schemes for a secured big data and cloud ICT framework in smart grid system. *Secur. Commun. Netw.* **2016**, *9*, 5262–5277.
78. Ullah, I.; Khan, M.A.; Abdullah, A.M.; Mohsan, S.A.H.; Noor, F.; Algarni, F.; Innab, N. A conditional privacy preserving generalized ring signcryption scheme for micro aerial vehicles. *Micromachines* **2022**, *13*, 1926.
79. Din, N.; Waheed, A.; Zareei, M.; Alanazi, F. An improved identity-based generalized signcryption scheme for secure multi-access edge computing empowered flying Ad Hoc networks. *IEEE Access* **2021**, *9*, 120704–120714.
80. Peng, X.; Zhang, J.; Zhang, S.; Wan, W.; Chen, H.; Xia, J. A secure signcryption scheme for electronic health records sharing in blockchain. *Comput. Syst. Sci. Eng.* **2021**, *37*, 265–281.
81. Wang, C.; Liu, C.; Li, Y.; Qiao, H.; Chen, L. Multi-message and multi-receiver heterogeneous signcryption scheme for ad-hoc networks. *Inf. Secur. J.* **2017**, *26*, 136–152.
82. Xiong, H.; Hou, Y.; Huang, X.; Zhao, Y.; Chen, C.-M. Heterogeneous signcryption scheme from IBC to PKI with equality test for WBANs. *IEEE Syst. J.* **2022**, *16*, 2391–2400.
83. Zhu, F.; Wu, W.; Abuadbbba, A.; Kumari, S.; Yang, X.; Khalil, I.; Yi, X. Lightweight privacy-friendly aggregation scheme against internal attacks for smart grids. *IEEE Trans. Ind. Inform.* **2025**, *21*, 4809–4819.
84. Thumbur, G.; Rao, G.S.; Reddy, P.V.; Gayathri, N.B.; Reddy, D.V.R.K. Efficient pairing-free certificateless signature scheme for secure communication in resource-constrained devices. *IEEE Commun. Lett.* **2020**, *24*, 1641–1645.
85. Huang, H.; Wu, Y.; Xiao, F.; Malekian, R. An efficient signature scheme based on mobile edge computing in the NDN-IoT environment. *IEEE Trans. Comput. Soc. Syst.* **2021**, *8*, 1108–1120.
86. Luo, M.; Zhou, X.; Qiu, M. A revocable anonymous cross-domain communication scheme for smart grid based on ring signcryption. *Peer- Netw. Appl.* **2024**, *17*, 125–138.
87. Yang, Y.; Zhang, L.; Zhao, Y.; Choo, K.-K.R.; Zhang, Y. Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based VANET. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 317–331.
88. Thorncharoensri, P.; Susilo, W.; Chow, Y.-W. Privacy-preserving file sharing on cloud storage with certificateless signcryption. *Theor. Comput. Sci.* **2022**, *916*, 1–21.

89. Shen, J.; Gui, Z.; Chen, X.; Zhang, J.; Xiang, Y. Lightweight and certificateless multi-receiver secure data transmission protocol for wireless body area networks. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 1464–1475.
90. Luo, M.; Zhou, Y. An efficient conditional privacy-preserving authentication protocol based on generalized ring signcryption for VANETs. *IEEE Trans. Veh. Technol.* **2022**, *71*, 10001–10015.
91. Ali, I.; Chen, Y.; Ullah, N.; Afzal, M.; He, W. Bilinear pairing-based hybrid signcryption for secure heterogeneous vehicular communications. *IEEE Trans. Veh. Technol.* **2021**, *70*, 5974–5989.
92. Niu, S.; Niu, L.; Yang, X.; Wang, C.; Jia, X. Heterogeneous hybrid signcryption for multi-message and multi-receiver. *PLoS ONE* **2017**, *12*, e0184407.
93. Yu, H.; Bai, L.; Hao, M.; Wang, N. Certificateless signcryption scheme from lattice. *IEEE Syst. J.* **2021**, *15*, 2687–2695.
94. Khanjari Mazrae, A.; Baghaee, H.R.; Sheikh-El-Eslami, M.K. Market-clearing mechanism in cyber-physical decentralized peer-to-peer energy trading: Insights into privacy and security vulnerabilities. *Sustain. Energy Grids Netw.* **2025**, *43*, 101914.
95. Hao, X.; Ren, W.; Choo, K.-K.R.; Xiong, N.N. A self-trading and authenticated roaming scheme based on blockchain for smart grids. *IEEE Trans. Ind. Inform.* **2022**, *18*, 4097–4106.
96. Hong, C.; Li, P.; Ma, H.; Yang, Y.; Zhou, X.; Liang, Z.; Zhou, D.; Zang, R. TrustPIoT: Blockchain-based anonymous authentication for cross-domain intelligent PIoT. In Proceedings of the 16th International Conference on Advanced Infocomm Technology (ICAIT), Enshi, China, 16–19 August 2024; pp. 284–289.
97. Tong, F.; Chen, X.; Wang, K.; Zhang, Y. CCAP: A complete cross-domain authentication based on blockchain for internet of things. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 3789–3800.
98. Wang, L.; Tian, Y.; Zhang, D. Toward cross-domain dynamic accumulator authentication based on blockchain in internet of things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2858–2867.
99. Wang, M.; Rui, L.; Yang, Y.; Gao, Z.; Chen, X. A blockchain-based multi-ca cross-domain authentication scheme in decentralized autonomous network. *IEEE Trans. Netw. Serv.* **2022**, *19*, 2664–2676.
100. Kaur, K.; Kaddoum, G.; Zeadally, S. Blockchain-based cyber-physical security for electrical vehicle aided smart grid ecosystem. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 5178–5189.
101. Xue, L.; Huang, H.; Xiao, F.; Wang, W. A cross-domain authentication scheme based on cooperative blockchains functioning with revocation for medical consortiums. *IEEE Trans. Netw. Serv.* **2022**, *19*, 2409–2420.
102. Abbasinezhad-Mood, D.; Ghaemi, H. Dual-signature blockchain-based key sharing protocol for secure V2V communications in multi-domain IoV environments. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 13407–13416.
103. Feng, C.; Liu, B.; Guo, Z.; Yu, K.; Qin, Z.; Choo, K.-K. R. Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones. *IEEE Internet Things J.* **2022**, *9*, 6224–6238.
104. Cheng, G.; Chen, Y.; Deng, S.; Gao, H.; Yin, J. A blockchain-based mutual authentication scheme for collaborative edge computing. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 146–158.
105. Erdayandi, K.; Cordeiro, L.C.; Mustafa, M.A. Privacy-preserving and accountable billing in peer-to-peer energy trading markets with homomorphic encryption and blockchain. *Sustain. Energy Grids Netw.* **2025**, *41*, 101560.
106. Liu, B.; Wu, J.; Chai, L. Distributed privacy-preserving algorithm for economic dispatch and demand response of smart grid with homomorphic encryption. *IEEE Trans. Smart Grid* **2025**, *16*, 173–182.
107. Zhao, J.; Zhang, Z.; Yu, H.; Ji, H.; Li, P.; Xi, W. Cloud-edge collaboration-based local voltage control for DGs with privacy preservation. *IEEE Trans. Ind. Inform.* **2023**, *19*, 98–108.
108. Dong, C.; Weng, J.; Liu, J.N.; Yang, A.; Liu, Z.; Yang, Y.; Ma, J. Maliciously secure and efficient large-scale genome-wide association study with multi-party computation. *IEEE Trans. Dependable Secur. Comput.* **2023**, *20*, 1243–1257.
109. Li, T.; Liu, W.; Xie, S.; Dong, M.; Ota, K.; Xiong, N.N.; Li, Q. BPT: A blockchain-based privacy information preserving system for trust data collection over distributed mobile-edge network. *IEEE Internet Things J.* **2022**, *9*, 8036–8052.
110. Guan, Z.; Zhou, X.; Liu, P.; Wu, L.; Yang, W. A blockchain-based dual-side privacy-preserving multiparty computation scheme for edge-enabled smart Grid. *IEEE Internet Things J.* **2022**, *9*, 14287–14299.
111. Mu, C.; Ding, T.; Sun, Y.; Huang, Y.; Li, F.; Siano, P. Energy block-based peer-to-peer contract trading with secure multi-party computation in nanogrid. *IEEE Trans. Smart Grid* **2022**, *13*, 4759–4772.
112. Huang, H.; Xue, S.; Zhao, L.; Wang, W.; Wu, H. Privacy-preserving smart energy management by consumer-electronic chips and federated learning. *IEEE Trans. Consum. Electr.* **2024**, *70*, 2200–2209.
113. Wang, Y.; Jia, M.; Gao, N.; Von Krannichfeldt, L.; Sun, M.; Hug, G. Federated clustering for electricity consumption pattern extraction. *IEEE Trans. Smart Grid* **2022**, *13*, 2425–2439.
114. Zhu, H.; Wang, R.; Jin, Y.; Liang, K. PIVODL: Privacy-preserving vertical federated learning over distributed labels. *IEEE Trans. Artif. Intell.* **2023**, *4*, 988–1001.
115. Liu, Z.; Hu, C.; Li, R.; Xiang, T.; Li, X.; Yu, J.; Xia, H. A privacy-preserving outsourcing computing scheme based on secure trusted environment. *IEEE Trans. Cloud Comput.* **2023**, *11*, 2325–2336.

116. Wang, J.; Wang, J.; Fan, C.; Yan, F.; Cheng, Y. SvTPM: SGX-based virtual trusted platform modules for cloud computing. *IEEE Trans. Cloud Comput.* **2023**, *11*, 2936–2953.
117. Zhang, F.; Zhang, Y.; Zhang, X. Desensitization method of meteorological data based on differential privacy protection. *J. Clean. Prod.* **2023**, *389*, 136117.
118. Xiang, N.; Zhang, X.T.; Dou, Y.; Xu, X.Q.; Yang, K.W.; Tan, Y. High-end equipment data desensitization method based on improved stackelberg GAN. *Expert Syst. Appl.* **2021**, *180*, 114989.
119. Wu, L.; Qin, C.; Xu, Z.; Guan, Y.; Lu, R. TCPP: Achieving privacy-preserving trajectory correlation with differential privacy. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 4006–4020.
120. Murakami, T.; Sei, Y. Automatic tuning of privacy budgets in input-discriminative local differential privacy. *IEEE Internet Things J.* **2023**, *10*, 15990–16005.
121. Wei, J.; Lin, Y.; Yao, X.; Zhang, J. Differential privacy-based location protection in spatial crowdsourcing. *IEEE Trans. Serv. Comput.* **2022**, *15*, 45–58.
122. von der Heyden, J.; Schlueter, N.; Binfet, P.; Asman, M.; Zdrallek, M.; Jager, T.; Darup, M.S. Privacy-preserving power flow analysis via secure multi-party computation. *IEEE Trans. Smart Grid.* **2025**, *16*, 344–355.
123. Fernando A, V.; Mithaguru; Lakshmanan, M.; Naik, M.N.; R, S.; Saxena, S. Federated learning for smart grid energy forecasting: A privacy-preserving approach. In Proceedings of the 2026 International Conference on Next-Gen Quantum and Advanced Computing: Algorithms, Security, and Beyond (NQComp), Bangalore, India, 5–6 March 2026; pp. 37–42.
124. Sultan, A.; Tahir, S.; Tahir, H.; Anwer, T.; Khan, F.; Rajarajan, M. A novel image-based homomorphic approach for preserving the privacy of autonomous vehicles connected to the cloud. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 1936–1948.
125. Zuo, X.; Li, L.; Peng, H.; Luo, S.; Yang, Y. Privacy-preserving multidimensional data aggregation scheme without trusted authority in smart grid. *IEEE Syst. J.* **2021**, *15*, 395–406.
126. Zhan, Y.; Zhou, L.; Wang, B.; Duan, P.; Zhang, B. Efficient function queryable and privacy preserving data aggregation scheme in smart grid. *IEEE Trans. Parallel Distrib. Syst.* **2022**, *33*, 3430–3441.
127. Xia, Z.; Zhang, Y.; Gu, K.; Li, X.; Jia, W. Secure multi-dimensional and multi-angle electricity data aggregation scheme for fog computing-based smart metering system. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 313–328.
128. Merad-Boudia, O.R.; Senouci, S.M. An efficient and secure multidimensional data aggregation for fog-computing-based smart grid. *IEEE Internet Things J.* **2021**, *8*, 6143–6153.
129. Wu, K.; Pan, J.; Zhang, Y. Power data aggregation method based on improved paillier homomorphic encryption. In Proceedings of the 8th International Conference on Electrical, Mechanical and Computer Engineering (ICEMCE), Xi'an, China, 25–27 October 2024; pp. 653–656.
130. Chen, D.; Zhou, T.; Liu, W.; Li, R.; Wu, L.; Yang, X. MDA-FLH: Multidimensional data aggregation scheme with fine-grained linear homomorphism for smart grid. *IEEE Internet Things J.* **2024**, *11*, 3524–3538.
131. Liang, W.; Yang, Y.; Yang, C.; Hu, Y.; Xie, S.; Li, K.C.; Cao, J. PDPChain: A Consortium blockchain-based privacy protection scheme for personal data. *IEEE Trans. Reliab.* **2023**, *72*, 586–598.
132. Ganjavi, R.; Sharafat, A.R. Edge-assisted public key homomorphic encryption for preserving privacy in mobile crowdsensing. *IEEE Trans. Serv. Comput.* **2023**, *16*, 1107–1117.
133. Sun, B.; Dang, Q.; Qiu, Y.; Yan, L.; Du, C.; Liu, X. Blockchain privacy data access control method based on cloud platform data. *Intl. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 10–18.
134. Halder, S.; Conti, M. CrypSH: A novel IoT data protection scheme based on BGN cryptosystem. *IEEE Trans. Cloud Comput.* **2022**, *10*, 2437–2450.
135. Jin, X.; Zhang, H.; Li, X.; Yu, H.; Liu, B.; Xie, S.; Singh, A.K.; Li, Y. Confused-modulo-projection-based somewhat homomorphic encryption—Cryptosystem, library, and applications on secure smart cities. *IEEE Internet Things J.* **2021**, *8*, 6324–6336.
136. Xiong, L.; Dong, D.; Xia, Z.; Chen, X. High-capacity reversible data hiding for encrypted multimedia data with somewhat homomorphic encryption. *IEEE Access* **2018**, *6*, 60635–60644.
137. Gentry, C. *A Fully Homomorphic Encryption Scheme*; Stanford University: Stanford, CA, USA, 2009; Volume 20.
138. Brakerski, Z.; Gentry, C.; Vaikuntanathan, V. (Leveled) fully homomorphic encryption without bootstrapping. *ACM Trans. Comput. Theory* **2014**, *6*, 1–36.
139. Fan, J.; Vercauteren, F. Somewhat practical fully homomorphic encryption. *Cryptol. ePrint Arch.* **2012**.
140. Cheon, J.H.; Kim, A.; Kim, M.; Song, Y. Homomorphic encryption for arithmetic of approximate numbers. In *Advances in Cryptology—ASIACRYPT 2017*; Springer: Cham, Switzerland, 2017; pp. 409–437.
141. Chillotti, I.; Gama, N.; Georgieva, M.; Izabachène, M. TFHE: Fast fully homomorphic encryption over the torus. *J. Cryptol.* **2020**, *33*, 34–91.
142. Li, R.; Ishimaki, Y.; Yamana, H. Fully homomorphic encryption with table lookup for privacy-preserving smart grid. In Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP), Washington, DC, USA, 12–15 June 2019; pp. 19–24.

143. Bao, J.; Zhang, Y.; Liu, H.; Li, Y.; Qiu, R. MIBFHE: Multi-identity fully homomorphic encryption for edge data sharing and cooperative computation. *Int. J. Netw. Secur.* **2022**, *24*, 342–351.
144. Castiglione, A.; Esposito, J.G.; Loia, V.; Nappi, M.; Pero, C.; Polsinelli, M. Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. *IEEE Trans. Ind. Inform.* **2025**, *21*, 1674–1683.
145. Teranishi, K.; Sadamoto, T.; Kogiso, K. Input–output history feedback controller for encrypted control with leveled fully homomorphic encryption. *IEEE Trans. Control Netw. Syst.* **2024**, *11*, 271–283.
146. Liu, Y.; He, Y.; Liu, Q.; Chen, Y.; Cai, Z. A flexible sharding blockchain protocol based on cross-shard Byzantine fault tolerance. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 2276–2291.
147. Deng, Z.; Tang, C.; Li, T.; He, D. Permissioned blockchain-based trusted and robust consensus optimization orienting intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2025**, *26*, 2011–2026.
148. Biswas, C.; Haque, M.M.; Das Gupta, U. A modified key sifting scheme with artificial neural network based key reconciliation analysis in quantum cryptography. *IEEE Access* **2022**, *10*, 72743–72757.
149. Noetzold, D.; Barbosa, J.L.V.; Paz, J.F.D.; Leithardt, V.R.Q. Reinforcement learning-based adaptive quantum-safe cryptography for DN25-compliant smart environments. *IEEE Access* **2026**, *14*, 62087–62104.

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.