ZWP-TRUST: Trusted Utility-Smart Telemetry Using Zero Knowledge Proofs, Reversible Watermarking, and Paillier Encryption

Tanya Koohpayeh Araghi*‡, Muhammad Yasir Masood*‡, Helena Rifà-Pous*‡, David Megías*‡,
Joan Ferré-Queralt †‡, Jordi Castellà-Roca†‡, Alexandre Viejo†‡

* Universitat Oberta de Catalunya (UOC)
UOC-TECH Research Center, Estudios de Informática, Multimedia y Telecomunicación
{tkoohpayeharaghi,mmasood,hrifa,dmegias}@uoc.edu
† Universitat Rovira i Virgili (URV)
Dept. d'Enginyeria Informàtica i Matemàtiques
{joan.ferreq,jordi.castella,alexandre.viejo}@urv.cat
‡ CYBERCAT - Center for Cybersecurity Research of Catalonia

***Abstract*—The innovation of smart grid technology poses very serious issues of data security and privacy to consumers, especially in the context of consumption data gathered by metering infrastructure. This paper proposes a high-frequency smart metering protocol that integrates homomorphic encryption, reversible watermarking, and zero-knowledge proofs to provide secure, privacy-preserving, and verifiable energy reporting. Reversible watermarking ensures the authenticity of the data while preserving the ability to fully recover the original measurements, and Paillier encryption enables aggregation directly over encrypted readings. To ensure the accuracy of meter-reported values, the protocol incorporates a Zero-Knowledge Proof (ZKP) mechanism that allows each smart meter to prove that its measurement lies within an allowed range without disclosing the actual reading. This prevents compromised meters from submitting malicious extreme values that could distort consumption data and disrupt grid operations. In general, the proposed protocol offers strong guarantees of integrity, confidentiality, and accountability while supporting the fine-grained reporting demands of modern smart grid infrastructures.**

***Index Terms*—smart grid, privacy, security, reversible watermarking, zero-knowledge proofs, Paillier encryption**

I. Introduction

The emergence of smart grid technology has reshaped how electricity is generated, distributed, and exchanged [1]. By combining power systems with advanced communication and control technologies, smart grids enable a more efficient, flexible, and resilient energy infrastructure. This evolution is driven by the growing penetration of renewable sources, the need for a stable supply, and the pursuit of sustainability and energy efficiency [2]. Beyond improving reliability, smart grids foster decentralized energy markets where consumers can actively trade for electricity.

A key enabler of this paradigm is the deployment of distributed energy resources (DERs) such as solar panels, wind turbines, and storage units located near consumption points [3]. These systems allow prosumers to both generate and consume energy, supporting bidirectional flows of power and information that make real-time trading and dynamic pricing possible [4]. A prosumer is a consumer who both consumes and produces electricity, most often using renewable energy sources such as solar panels or wind turbines. Prosumers can also store energy and inject surplus energy into the grid, becoming active energy market players as opposed to being passive consumers of energy [5]. Such interactivity enhances load balancing and the integration of renewable energy across the grid.

However, as energy trading becomes increasingly decentralized, new challenges arise concerning security, privacy, and scalability. Advanced metering infrastructure (AMI) supports real-time monitoring and optimization but also exposes detailed consumption data. Through *user profiling*, an attacker could infer private information about consumers' habits and routines. Ensuring data confidentiality is therefore vital to protect privacy and maintain trust in decentralized energy markets [6].

This paper introduces a high-frequency smart metering protocol that combines Paillier homomorphic encryption, reversible watermarking, and zero-knowledge proofs to secure and verify energy readings. The proposed protocol delivers confidentiality, integrity, and resilience for fine-grained smart grid data collection.

The rest of the paper is organized as follows: in Section II, the preliminaries on smart gird fundamentals and watermarking and cryptographic functions are explained. In Section III, recent related works in advanced metering system are described. Section IV introduces the proposed protocol and system entities. In Section V, The cryptography and data hiding fundamentals are described. The different phases of the proposed protocol are explained in Section VI. Evaluation and analysis, and comparison and discussion are described in Sections VII and VIII, and finally Section IX relates the conclusion and future work.

II. Preliminaries

This section presents the basic understanding on which decentralized energy trading is based in smart grids. We start with a definition of the smart grid itself and introduce its main elements: Distributed Energy Resources (DERs) and the place of consumers [7]. Lastly, we explain what is known as the

Advanced Metering Infrastructure (AMI) that allows the real-time, data-driven operations, which despite its advantages, raises serious security and privacy issues.

A. Smart Grid Fundamentals

A traditional power grid is taking the form of a smart grid, which is arguably defined as a modernized electrical power grid that employs information and communication technology (ICT) to detect and respond to data in an automated manner [8]. This is because this integration makes the generation, distribution, and consumption of electricity more efficient, reliable, and sustainable. The smart grid is not a technology but a web of systems, and there are two-way flows of electricity and information, which allow the introduction of new functionalities, such as real-time monitoring, dynamic pricing, and better fault handling.

B. Distributed Energy Resources (DERs)

One of the foundations of the smart grid is the spread of the DERs. DERs refer to miniature power generation/ storage devices (e.g., rooftop solar panels, mini wind turbines, battery storage) that are situated within the proximity to the point of electricity usage [7]. This decentralization enables the end-users to be consumers who consume and generate energy. Consumers are able to produce electricity that they can use themselves and feed the excess into the grid. Such an ability establishes two-way power flows, essentially altering the passivity of the traditional energy consumers and opening the door to peer-to-peer energy trading and the creation of decentralized energy markets.

C. Advanced Metering Infrastructure (AMI)

The AMI enables the flow of information in both directions required to make smart grid operations possible. AMI is an all-inclusive system of smart meters (SMs), communication networks, and data management systems that allows two-way communication between utilities and consumers [9]. SMs, the important element of AMI, are used to gather detailed and high-frequency energy consumption data (as well as generation, in the case of prosumers). This information is delivered in close real-time, and it is possible to:

- Dynamic Pricing: Implementing time-of-use rates and real-time pricing.
- Real-time Monitoring: Provide utilities with a precise view of grid conditions.
- Demand Response: Allowing utilities to manage load by incentivizing reduced consumption during peak periods.

Although privacy and confidentiality deal with the fact that the consumption data has not been revealed to an unauthorized individual, integrity addresses the fact that the metering and control information is accurate and untouched. In the further discussion, however, the threat shifts to the issues of integrity in the smart grid setting. The granular data of consumption, which AMI has accumulated, is, however, a two-edged sword. Although it is critical to optimize a grid, it may be profiled by a user, in which attackers can use the data to deduce personal information about a consumer, his or her habits, routines, and even the use of appliances. Securing this information is, hence, a serious problem with decentralized energy trading systems.

The main security concern of AMI is to make sure that no one has altered consumption data throughout the transmission, and the origin of the consumption data can be verified. The reversible watermarking has been one of the tools that pays off and addresses the issue without affecting the utility of the data [10].

D. Reversible Watermarking

Digital watermarking is essentially the process of embedding hidden information, known as a watermark, within original data to enable tamper detection, copyright protection and authentication verification. The watermark bits should be dispersed across the host data in such a way that they cannot be easily detected. The embedding process must preserve the logical integrity of the original information, and a corresponding algorithm should be capable of extracting the embedded watermark. Furthermore, digital watermarking methods do not introduce extra communication costs or processing overhead and are generally lighter than cryptographic approaches, making them suitable for resource-limited sensor devices [11].

Reversible or lossless digital watermarking refers to methods that not only verify the authenticity of protected data but also allow the exact recovery of the original sensed information. Traditional non-reversible watermarking cannot completely recover the original data once an attack has occurred. Although it introduces only slight data alterations, these modifications are permanent. Therefore, for applications that require high accuracy, such as in military, medical, or smart metering systems, non-reversible watermarking is unsuitable. Consequently, reversible digital watermarking is considered the most appropriate technique for IoT sensor networks [12].

The core strength of this approach is its perfect reversibility. After receiving the watermark data and the command for the integrity of the data, the utility can run the extraction algorithm to discard the watermark and recover the exact original consumption values [13].

This is essential for regulatory compliance and accurate billing as it prevents any long-term distortion of the foundational data. More recent research has tailored these algorithms to the smart grid environment, so that it is not only small enough to execute on the limited hardware of a standard meter, but also hardened enough to resist undetectable and non-removable tampering. Thus, through reversible watermarking, the utilities will be able to leverage the entire potential of AMI to guarantee the authenticity of the data, as well as create a two-way communication environment where they can ensure the accuracy of the consumption data as it will eventually be required in the final critical uses [14].

E. Paillier Encryption

The proposed model is based on the Paillier cryptosystem, which is a probabilistic asymmetric encryption scheme characterized by the additive homomorphic property. This special property enables certain computations to be done on ciphertexts; two ciphertexts, when decrypted, give back the sum of their plaintexts [15]. This functionality offers unique features in our proposed architecture. To begin with, it allows the lightweight SMs to concentrate on reversible watermarking only and leave the more resource-intensive

Pallier encryption to the dedicated Encryption Server (ES). Secondly, and most importantly, it allows the creation of an aggregation that preserves privacy [16]. Data Aggregator (DA) is able to calculate cumulative consumption by multiplying encrypted readings of multiple SMs without the need to decrypt them, so that the data regarding households is kept secret. Lastly, the scheme offers end-to-end confidentiality in the transmission, where the data is encrypted between the ES and the Control Center (CC), which finally decrypts the data. This process has its security based on the intractable Decisional Composite Residuality Assumption (DCRA) . The Paillier cryptosystem would make up a bottom layer together with the zero-knowledge proofs of the Billing Server (BS), which establishes the validity of the data, without showing the data, and balanced the requirement of the utility to do accurate aggregation and the requirement of consumer privacy [17].

III. Related Works

Advanced Metering Infrastructure is a technology that has radically changed the traditional electrical grids into data-driven networks. Although such a shift enables the implementation of crucial features such as demand response and remote control, it also raises complicated issues such as information protection, data integrity, and consumer privacy [18]. The consumption information that Smart Meters (SMs) gather on a fine-grained basis has the potential to depict very sensitive occupancy trends and individual habits, posing a serious risk to privacy [19]. Moreover, the data, upon which such critical operations as correct billing and grid balancing are based, should be reliably justified and guarded against malicious interference. To resolve both of these issues, integrity and confidentiality require the combined use of cryptography, and this is what contemporary texts discuss [20]. The fundamental security issue that AMI faces is the integrity of the data; that is, ensuring that the data on consumption has not been distorted in transit and that it is actually authentic. Reversible Watermarking (RW) has become a very effective method that can address this issue without hurting the usefulness of the original data negatively [10]. Techniques such as Prediction-Error Expansion (PEE) have been employed by researchers, leveraging the natural correlation between sequential meter readings to implement authentication codes directly within the data stream, particularly Hash-based Message Authentication Codes (HMACs), as seen in studies like [21] on lightweight authentication. This is the key characteristic that makes RW stand out from unidirectional approaches: having verified the integrity, it is possible to reconstruct the original meter data with 100 percent accuracy. This feature does away with the conventional trade-off between data accuracy and security fidelity, the key to billing and forensic analysis. Nonetheless, reversible watermarking is not fraud-proof against the central utility or possible third-party eavesdroppers, even though it does guarantee the integrity of the data. The threat of infringement of privacy as a result of the analysis of a detailed load profile must be investigated with regard to encryption techniques capable of maintaining functionality. The Paillier Cryptosystem is famously considered a formidable application in this field since it possesses the distinctive additive homomorphic property of a cryptography system [5]. This mathematical property permits the use of operations on the encrypted ciphertexts to be directly related to additions on the plaintext domain on decryption. This principle was modified to be used in aggregation in the Smart Grid, which was initially proposed by Garcia and Jacobs, who suggested an architecture that has SMs that encrypt their readings using a public key. The Data Aggregator can then determine the accumulated consumption by a collection of households by just multiplying the individual ciphertexts. The result of the decryption of this product is only the total value, which, in essence, hides the information about any individual home. This model is very useful in reducing the leakage of data without interfering with the computational ability of grid monitoring that is needed in grid monitoring and control systems [22]. Paillier encryption is based upon the computational hardness of the Decisional Composite Residuosity Assumption (DCRA), which offers a solid mathematical foundation to resist eavesdropping. Since reversible watermarking and Paillier encryption solve two orthogonal security concerns (integrity versus privacy), the literature implies that the two synergize well and are needed to do so. The most holistic security solutions adopt a hybrid scheme, in which data is first encrypted by Paillier to obscure consumption patterns to interceptors and a reversible watermark is added (or it can be found in the SM) to add a layer of integrity checking and authentication, still verifiable even in the encrypted space. This multi-level design can ensure data privacy as well as data integrity at every stage of the transmission channel, which meets the multifaceted and multidimensional security requirements of a smart grid of the modern world [23]. Recent studies, especially protocols like the ReWaP: Reversible Watermarking and Paillier Encryption Approach to Privacy-preserving Smart Meter [20] and similar works on Privacy-preserving protocols to high-frequency smart meters, have focused on how best these techniques can be combined to provide computationally lightweight and robust solutions that can run in resource-constrained SM environments.

IV. Proposed Model

The proposed model introduces a secure Privacy-Preserving Protocol for SMs designed to secure smart grid data through a joint application of difference expansion-based reversible watermarking and Paillier homomorphic encryption. This hybrid method aims to maintain privacy and data integrity while being computationally efficient for resource-constrained SMs that transmit readings every few seconds or minutes. In the following, the system model and each entity are introduced.

A. System Model and Entities

The system architecture consists of four main entities.

1. Smart Meters (SMs): Installed at user premises, responsible for energy measurement and initial watermark embedding. SMs can be corrupted and used to report malicious values. The typical goal of such an attack is to inject extreme (very large or very small) readings so as to significantly bias the final aggregated result and, in turn, disrupt grid operations or downstream decision processes.

2. Encryption Server (ES): A lightweight intermediary performing Paillier encryption to reduce computation on SMs.

3. Data Aggregator (DA): Collects encrypted data from multiple SMs and performs aggregation in the encrypted domain.

4. Control Center (CC): Performs decryption, watermark verification, and data aggregation analysis.

5. Billing Server (BS): The entity in charge of billing and customer invoicing. In many practical deployments the BS already collects fine-grained (per-customer) meter readings for invoicing and commercial purposes. In this extended model the BS can locally generate a cryptographic proof that a reported smart-meter reading lies within a given interval $[L, U]$ (a *zero-knowledge proof*) without disclosing the exact reading to other parties. However, this entity must not know from which exact user the reading is to further protect the privacy.

This model assumes that at most one of the entities (ES, DA, CC) could be compromised at a time, ensuring multi-layer defense even if a single layer is breached.

V. Cryptographic and Data-Hiding Foundations

In the following the cryptographic technology and type of the used watermarking scheme is explained.

A. Reversible Watermarking via Difference Expansion

Reversible watermarking ensures both authentication and integrity by embedding binary watermarks into data without loss of the original content.

Watermark Generation: A binary watermark is generated using SHA-2 hash values derived from the secret key $\mathsf{K_w}$ and timestamps.

Watermark Embedding: The watermark bit is embedded in the least significant bit of the difference between two consecutive measurements.

Watermark Extraction: After decryption, the original readings and watermark can be perfectly recovered, ensuring the accuracy and verification of the integrity of the data.

B. Paillier Cryptosystem

The Paillier encryption scheme provides additive homomorphism, allowing the DA to aggregate encrypted values directly without decryption. This ensures:

- Aggregation of consumption data without revealing individual readings.
- End-to-end confidentiality during communication.

C. Zero-Knowledge Proofs (ZKPs)

Zero-knowledge proofs allow a prover to convince a verifier that a statement is true without revealing any information beyond its validity.

Private Inputs: The prover holds a secret value, or witness, that satisfies a public statement. This value remains hidden throughout the protocol.

Public Inputs: These are the parameters and statements known to both parties, such as cryptographic commitments, encrypted values, or claimed properties to be verified.

Prover and Verifier Roles: The prover constructs a proof demonstrating knowledge of a valid witness for the public statement, while the verifier checks the proof's correctness without learning the witness itself.

Zero-knowledge proofs thus ensure verifiable correctness of computations or claims while preserving the privacy of the underlying data.

VI. Protocol Workflow

The proposed protocol consists of five sequential phases:
Primary Setup and Initialization:

- The CC distributes a secret key $\mathsf{K_w}$ and pseudo-random number generator (PRNG) seeds to all SMs via secure bootstrapping.
- Paillier key pairs are generated by the CC, while only the public key is shared with the ES.
- Each SM initializes three PRNGs to generate different random numbers for encryption and obfuscation at each timestamp.

Phase 1 — Watermark Embedding:

- Each SM embeds a watermark bit using difference expansion in two consecutive readings.
- The watermarked values are obfuscated with pseudo-random numbers.
- The readings, the watermark and the pseudo-random numbers are sent to the BS via a secure and confidential mixing protocol between the home SMs so that the BS is not able to know to whom the readings belong.

Phase 2 - Proof Generation at BS:

- BS generates a zk-proof with private inputs (readings, watermark, pseudo-random numbers) and public inputs (lower bound, upper bound). It proves that the readings are both between a certain range without revealing them.
- Sends proof back to SM.

Phase 3 - Local Encryption at SM:

- The obfuscated watermarked values are XOR-encrypted before transmission to the ES along with the proof.

Phase 4 — Paillier Encryption at ES:

- ES decrypts the XOR layer and verifies the proof.
- If correct, ES performs Paillier encryption on the watermarked data using the CC's public key.
- The ciphertexts are re-encrypted via XOR for secure transmission back to the SM.

Phase 5 — Re-encryption and Forwarding:

- SMs decrypt and re-encrypt the Paillier ciphertexts with a different PRNG key before sending them to the DA.

Phase 6 — Data Aggregation at DA:

- DA decrypts the XOR layer and aggregates the Paillier ciphertexts from all SMs homomorphically, forwarding the aggregated results to CC.

Phase 7 — Verification and Decryption at CC:

- CC decrypts the aggregated data, removes pseudo-random obfuscation, and extracts the watermark.
- If the extracted watermark matches the expected one, the data is verified as authentic; otherwise, it is flagged as tampered.

The design of the system ensures that even if any intermediary (ES or DA) is compromised, neither fine-grained user data nor valid watermarks can be reconstructed.

Figure 1 shows the details of the proposed model

VII. Evaluation and Analysis

A set of theorems formally prove that the proposed protocol satisfies the essential data and privacy requirements. They are described as follows:

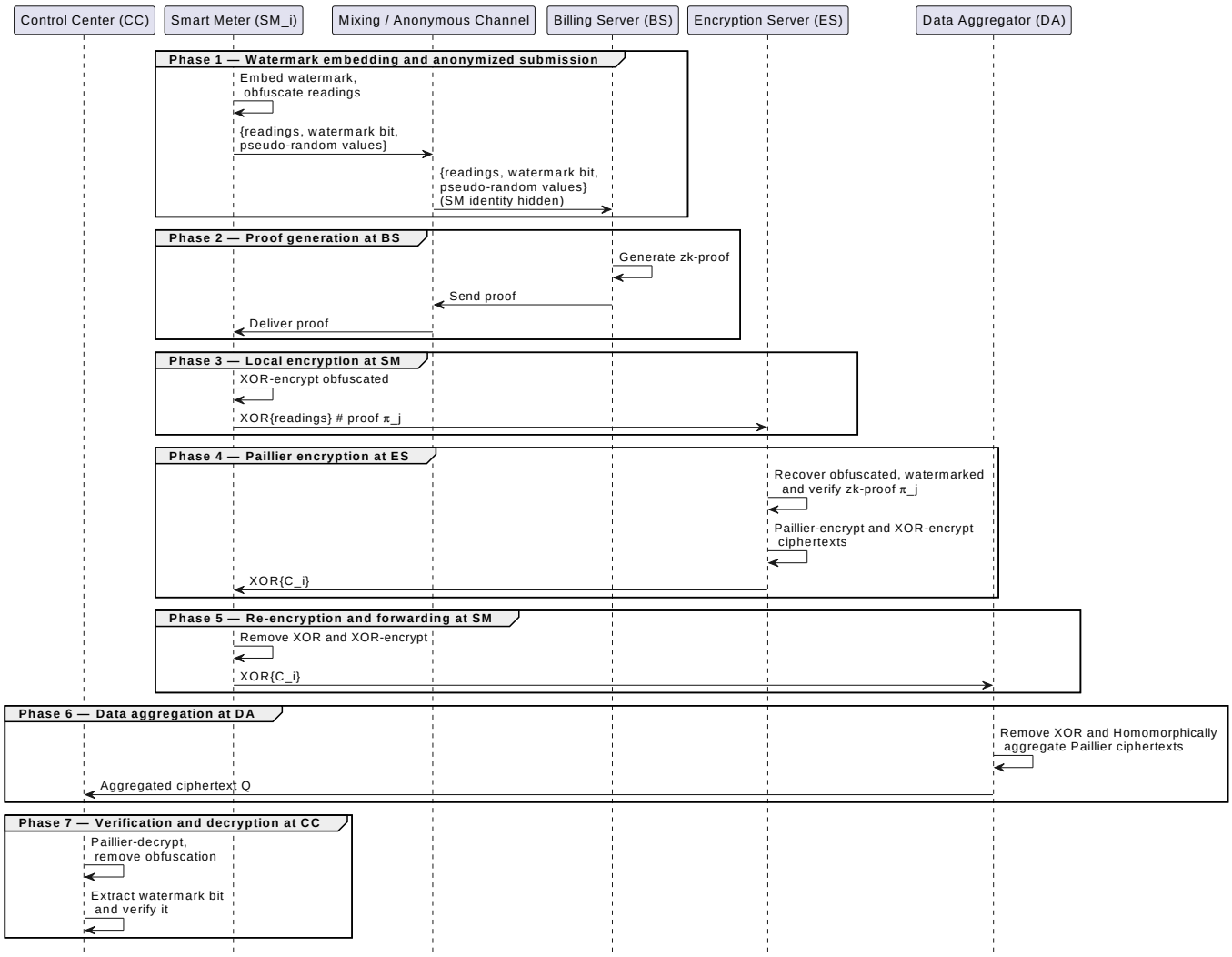


Figure 1. Protocol Phases

Privacy: Individual fine-grained data remain hidden from unauthorized entities.

Accuracy: Homomorphic aggregation guarantees that decrypted totals match the true sum of all users' consumption.

Confidentiality and Integrity: Reversible watermarking ensures tamper detection; data cannot be altered undetected.

Attack Resistance:

- *Eavesdropping and Man in the Middle (MitM) attacks:* Multi-level encryption and pseudo-random masking render intercepted data meaningless.
- *Masquerading and Replay attacks:* Unique PRNG sequences and timestamps invalidate repeated or forged transmissions.
- *False Data Injection (FDI):* Any tampering alters the watermark, triggering detection.
- *Data Poisoning:* A corrupt SM is not able to poison the aggregated sum with extreme values, the zk-proofs guarantees that the readings are between a certain range.

Table I shows the summary of defense mechanism result.

Table I
DEFENSE MECHANISM RESULT.

Attack Type	Defense Mechanism	Result
Eavesdropping	XOR + Paillier Encryption	Data unreadable
MITM	Watermark verification	Tampering detected
Replay	Timestamp validation	Data discarded
Masquerading	Unique PRNG seeds	Forgery prevented
FDI	Watermark mismatch	Fake data rejected
Data Poisoning	Zero-knowledge proofs	Range verified

VIII. COMPARISON AND DISCUSSION

In this section, the proposed model is compared with several recent models. Table II shows that the proposed model meets all the security and privacy requirements of fine-grained metering data compared to recent models.

Table II
COMPARISON OF SECURITY AND PRIVACY REQUIREMENTS

Methods	ReWap [20]	PFDAM [24]	EPri-MDAS [25]	NHP^3 [26]	Proposed Model
User Privacy	√	√	√	×	√
Accuracy	√	×	×	×	√
Confidentiality	√	√	√	√	√
Integrity	√	√	√	√	√

We also compared the resistance of our proposed model against the most common attacks that endanger the smart metering system with recent models. This comparison shows that the proposed model represents superiority in the detection

Table III
COMPARISON OF ATTACK RESISTANCE

Methods	ReWap [20]	PFDAM [24]	EPri-MDAS [25]	NHP^3 [26]	Proposed Model
Eavesdropping	√	√	√	√	√
MitM	√	√	√	×	√
Masquerading	√	×	×	×	√
Replay	√	√	√	×	√
FDI	√	√	√	√	√
Data Poisoning	×	×	×	×	√

and prevention of attacks compared to the other proposed models. Table III shows the comparison of the robustness of the proposed scheme with several recent methods.

IX. CONCLUSION AND FUTURE WORK

The proposed protocol provides a unified security framework for high-frequency smart that strengthens confidentiality, integrity, and verifiability in high-frequency smart metering. By combining reversible watermarking, Paillier homomorphic encryption, and ZKPs, it ensures that fine-grained readings remain private while still enabling accurate aggregation and robust tamper detection. The layered architecture enhances efficiency by delegating Paillier operations to a dedicated encryption server, reducing computational load on smart meters. Reversible watermarking guarantees integrity, authentication, and full recovery of original readings, which is essential for accurate billing and regulatory compliance. Homomorphic aggregation preserves end-to-end confidentiality while enabling accurate system-wide analytics. ZKPs generated at the billing server ensure that each reading lies within an admissible range without revealing its value, providing strong protection against data-poisoning attacks. Formal analysis confirms resistance against eavesdropping, replay, masquerading, and data-poisoning attacks, while maintaining full recoverability of original measurements for billing and regulatory needs. Future work will evaluate the scalability of the architecture in large deployments and analyse the performance overhead of ZKP generation and verification.

ACKNOWLEDGMENTS

This research is supported by Projects HERMES, DANGER and ARTEMISA, funded by the European Union NextGenerationEU/PRTR via INCIBE; by Projects PID2021-125962OB-C31 “SECURING/CYBER”, PID2021-125962OB-C32 “SECURING/DATA”, PID2024-156914OB-C41 “SAFE/CYBER” and PID2024-156914OB-C42 “SAFE/DATA”, funded by MCIN/AEI/10.13039/501100011033; and by Grant SGR2021-00115, funded by AGAUR, Generalitat de Catalunya. Joan Ferré-Queralt is supported by the Spanish Government under an FPU grant (ref. FPU23/01275). Alexandre Viejo is a Serra-Húnter Fellow.

REFERENCES

[1] C. W. Gellings, *The smart grid: Enabling energy efficiency and demand response*. CRC press, 2009.

[2] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart grid—the new and improved power grid: A survey,” *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[3] C. Liu, Y. Zhou, Z. Zhao, H. Tian, Y. Zhang, and Z. Cai, “Cyber security and privacy issues in smart grids,” *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.

[4] Y. Parag and B. K. Sovacool, “Electricity markets design for the prosumer era,” *Nature Energy*, vol. 1, no. 4, p. 16032, 2016.

[5] B. Liu, J. Wu, and L. Chai, “Distributed privacy-preserving algorithm for economic dispatch and demand response of smart grid with homomorphic encryption,” *IEEE Transactions on Smart Grid*, 2024.

[6] A. R. Metke and R. L. Ekl, “Security technology for smart grid networks,” in *Proceedings of the IEEE*, vol. 98. IEEE, 2010, pp. 2–5.

[7] S. Habib, “Robust load and energy management in smart grids with prosumer-integrated distributed energy resources,” *Journal of Cleaner Production*, vol. 496, p. 145138, 2025.

[8] B. N. Alhasnawi, H. K. Hashim, M. Zanker, and V. Bureš, “The rising, applications, challenges, and future prospects of energy in smart grids and smart cities systems,” *Energy Conversion and Management: X*, p. 101162, 2025.

[9] N. Amuthan, M. Sathya, and N. C. Rani, “Empowering consumers and utilities for a smarter future: The pivotal role of advanced metering infrastructure (ami) in smart meter technology,” *Cloud Computing in Smart Energy Meter Management*, pp. 31–65, 2025.

[10] Z. Song, A. Skuric, and K. Ji, “A recursive watermark method for hard real-time industrial control system cyber-resilience enhancement,” *IEEE Transactions on Automation Science and Engineering*, vol. 17, no. 2, pp. 1030–1043, 2020.

[11] T. K. Araghi, D. Megías, and A. Rosales, “Toward the selection of a lightweight authentication technique for the security of smart homes: Framework architecture based on a user centric design,” in *Intelligent Computing*, K. Arai, Ed. Cham: Springer Nature Switzerland, 2023, pp. 651–667.

[12] T. K. Araghi, D. Megías, and A. Rosales, “Evaluation and analysis of reversible watermarking techniques in wsn for secure, lightweight design of iot applications: A survey,” in *Future of Information and Communication Conference*. Springer, 2023, pp. 695–708.

[13] G. Kuldeep and Q. Zhang, “Multi-class privacy-preserving cloud computing based on compressive sensing for iot,” *Journal of Information Security and Applications*, vol. 66, p. 103139, 2022.

[14] J. Du, C. Dai, P. Mao, W. Dong, X. Wang, and Z. Li, “An efficient lightweight authentication scheme for smart meter,” *Mathematics*, vol. 12, no. 8, p. 1264, 2024.

[15] S. Zhao, “Smart grids data aggregation method on paillier homomorphic encryption,” *Applied Artificial Intelligence*, vol. 38, no. 1, p. 2327901, 2024.

[16] B. Qu, Z. Wang, B. Shen, H. Dong, and X. Zhang, “Secure particle filtering with paillier encryption–decryption scheme: Application to multi-machine power grids,” *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 863–873, 2023.

[17] F. Kabir, T. K. Araghi, and D. Megías, “Privacy-preserving protocol for high-frequency smart meters using reversible watermarking and paillier encryption,” *Computers and Electrical Engineering*, vol. 119, p. 109497, 2024.

[18] J. Sun, Y. Bao, W. Qiu, R. Lu, S. Zhang, Y. Guan, and X. Cheng, “Privacy-preserving fine-grained data sharing with dynamic service for the cloud-edge iot,” *IEEE Transactions on Dependable and Secure Computing*, 2024.

[19] P. Yu, W. Huang, and Z. Li, “A secure, lightweight, and verifiable data aggregation scheme for smart grids,” *Peer-to-Peer Networking and Applications*, vol. 18, no. 3, pp. 1–11, 2025.

[20] F. Kabir, K. Cabaj, T. K. Araghi, and D. Megías, “Rewap: Reversible watermarking and paillier encryption approach for privacy-preserving smart meter,” in *International Conference on Availability, Reliability and Security*. Springer, 2025, pp. 346–363.

[21] S. Kook, K. Kim, J. Ryu, Y. Lee, and D. Won, “Lightweight hash-based authentication protocol for smart grids,” *Sensors*, vol. 24, no. 10, p. 3085, 2024.

[22] H. Li, X. Li, and Q. Cheng, “A fine-grained privacy protection data aggregation scheme for outsourcing smart grid,” *Frontiers of Computer Science*, vol. 17, no. 3, p. 173806, 2023.

[23] M. Bakkar, S. Bogarra, F. Córcoles, J. Iglesias, and W. Al Hanaineh, “Multi-layer smart fault protection for secure smart grids,” *IEEE Transactions on Smart Grid*, vol. 14, no. 4, pp. 3125–3135, 2022.

[24] J. Zhang and J. Wei, “Pfdam: Privacy-preserving fine-grained data aggregation scheme supporting multifunctionality in smart grid,” *IEEE Internet of Things Journal*, vol. 11, no. 15, pp. 25 520–25 533, 2024.

[25] J. Zhang, W. Zhang, X. Wei, and H. Liu, “Epri-mdas: An efficient privacy-preserving multiple data aggregation scheme without trusted authority for fog-based smart grid,” *High-Confidence Computing*, vol. 4, no. 4, p. 100226, 2024.

[26] A. Mohammadali and M. S. Haghighi, “A privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance for metering data aggregation in smart grid,” *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5212–5220, 2021.