Answers to Reviewers

Please find below our answers to the *comments* from the three reviewers. The main changes/additions to the PDF file are also tracked in blue. Many thanks for these useful suggestions and comments.

Reviewer #1

Concern #1
In the abstract, a comparison is made between CHEA and existing methods, highlighting the advantages of CHEA. These results are meaningful; however, specific numerical values are lacking. It is recommended to briefly list these performance metrics in the abstract to provide readers with a more intuitive understanding of the improvements.

Author response: We appreciate the suggestion, but feel that including technical details in the abstract would lack the context necessary to interpret them. For this reason, we will avoid using timing or communication numbers in the abstract. However, we have added a more concrete security feature comparison that enhances the abstract based on your suggestion.

Author action: Updated abstract to reflect new analysis of security features.

Additionally, CHEA retains all standard security properties held by other aggregation schemes, while improving flexibility and reducing infrastructural requirements.

Concern #2
The paper mentions the existence of several solutions, but it does not provide a detailed explanation of the working principles and pros and cons of these solutions. It is advisable to conduct a more in-depth analysis and comparison of these solutions in the paper to help readers better understand the research background and contributions.

Author response: We have revised the related work section to better communicate the features and technical details of related solutions. Additionally, we added a table to facilitate a more concrete comparison of security and architectural features between relevant schemes.

Author action: Updated Section 3 with the inclusion of Table 2.

Concern #3
Various methods for processing energy usage data are mentioned in the paper, such as algebraic transformations, data aggregation, and random noise. It is recommended to provide more detailed explanations of the working principles and advantages and disadvantages of each method in the paper to help readers better understand the application scenarios of these methods.

Author response: We have updated the section on alternatives to provide more detailed technical explanations of each method. In addition, we introduced a new table that compares the features of each method to more clearly justify our selection of data aggregation as the base technique.

Author action: Updated Section 2 with the inclusion of Table 1.

Concern #4
The paper mentions the use of the Paillier homomorphic encryption system but does not provide information about why this system was chosen and comparisons with other homomorphic encryption systems. It is suggested to provide more detailed information about the implementation of homomorphic encryption and the rationale behind the selection in the paper.

Author response: The Paillier cryptosystem was chosen for its computational efficiency due to the processing limitations of AMI equipment. The article has been updated to reflect this rationale.

Author action: Updated Section 4:
This last property is essential due to the relatively weak processing power of AMI equipment.

Concern #5
The paper mentions the adjustment of parameters α and β but requires more information to explain how to determine the optimal parameter values for different application scenarios. It is recommended to provide guidance on parameter selection and examples of practical applications.

Author response: References supporting the value of variable subset sizing and an improved explanation of the parameters were included. As or parameter selection, this part is too context-specific for guidelines beyond Zhang and Liu [22] to be provided at this time

Author action: Updated Section 4:
The parameters α and β enable the DSO to dynamically adjust the level of aggregation as well as the precision of the aggregation regions. Zhang and Liu [22] note that variable subset sizes enable improved data analysis by the DSO. The capacity to target different regions and/or degrees of aggregation allows the scheme to support multiple privacy-preserving applications making use of aggregated data.

Concern #6
The paper mentions the use of two custom C programs for simulation experiments but needs to provide more detailed descriptions of the experiments so that readers can understand the specific process and settings. For example, more information can be provided about simulation parameters, input data, and experimental procedures.

Author response: Thanks for this comment. The purpose of the simulation should have been more clearly addressed; we hope that the new introduction of Section 6.3 (which augments previous short sections 6.3 and 6.4) improves the clarity of the work.

Author action: Updated Sections 6 & 6.3, and added new Figure 5.

Concern #7
The paper mentions performance comparisons with other solutions but needs to provide a more detailed description of the performance comparison metrics and methods. Readers need to understand how performance was measured and compared to evaluate the results.

Author response: Indeed, the results section lacked details. We have extended the depth of the explanation, thanks to the comment.

Author action: Updated Sections 6 & 6.2, and added new Figure 5.

Concern #8
In the performance results section, more explanations are needed to help readers understand why certain aspects of performance are poorer and how these differences affect the practical application of the protocol.

Author response: Thank you for the comment. It was discovered that our measurements for CHEA were overestimated due to including transmission times in the results (not to mention using a different crypto library). The results have been revised and appropriately updated, and explanations have been improved to reflect these.

Author action: Updated Section 6.

Concern #9
The authors think that the research of this paper cannot be considered strictly a performance improvement, but it improved flexibility, fault tolerance, and security .Please provide a detailed description of where improvements in flexibility, fault tolerance, and security are reflected.

Author response: These improvements are now outlined concretely in the related work section via the chart comparing related schemes.

Author action: Updated related work (Section 3) and included new Table 2.

Concern #10
In Section 6, the simulation results were compared with the results of the references in Tables 2 and 3. Please supplement whether the testing environment tested in this article is consistent with the testing environment in the references.

Author response: The nature of the testing environment and its relationship to the references should have been more clearly addressed in the article text. They are now.

Author action: Updated Section 6.

Concern #11
In Section 6, the DSO application acts as a server for the smart meters and generates and distributes the plan. Please provide information on how the parameters in the relevant algorithms are determined.

Author response: The parameters have been more clearly defined, particularly in Section 6.3.

Author action: Updated Section 6 and created Section 6.3.

Concern #12
The paper mentions the scalability of the protocol but needs to discuss the practical significance and impact of this feature in more detail. Readers need to understand how the protocol adapts to different scales of smart meter networks.

Author response: While scalability was briefly mentioned, this comment brought attention to the fact that it was not explored thoroughly. To resolve this, results from scalability testing were included and Section 6.3 was created to better organize the information.

Author action: Updated Section 6 and created Section 6.3.

Concern #13
The paper mentions that due to the lack of available hardware for testing, software simulation was used to conduct tests. However, the best approach is to test with real physical smart meters in a real environment. It is advisable to discuss more explicitly in the paper the impact of the lack of hardware testing and possible solutions.

Author response: The impact of the lack of hardware is discussed in the Limitations (Section 7). While we regret this setback, it should be noted that similar schemes in related work also use software simulations to validate their solutions. This is somewhat of a necessity, since most current generation AMI hardware is not capable of performing the necessary cryptographic operations, making hardware testing unrealistic at this time. We have updated the limitations section to reflect this.

Author action: Updated Section 7:
Due to the lack of available hardware for testing, the protocol was tested using a software simulation of a smart grid environment. Ideally this would have been tested in a more accurate setup using real, physical smart meters to demonstrate feasibility and gather data for prospective users. However, given that most current-generation AMIs are not capable of performing the necessary operations, it is difficult to test HE-based aggregation schemes in

practice at this time. As a result, related literature largely relies on software simulations, as we did.

Reviewer #2

Concern #1
The only question is if the results presented in Table 3 can be improved, but considering the conclusions part, there is a lot of that is planned to be improved.

Author response: Thank you for your comment. In fact, it was found that the comparison was ungenerous to CHEA since we were including transmission times in our calculations (and had used a different library for testing). The results have been regathered and revised.

Author action: Updated Section 6.

Reviewer #3

Concern #1
For electricity grid applications, which may be or become the most important for modern society, the power issue is minimal, as no permanent battery operation has to be taken into account. Leaving the increased computing power as a potential issue (however, it may be assumed that AMIs designed for the electricity grid may have a certain computing power reserve, as power consumption critical design tends to be more costly.

The possible extension to other distribution infrastructure, in particular water, but possibly also gas, is a challenging prospect (whereas gas may be on tis way out, the measurement of consumption may therefore be even more critical)

Author response: Thank you for these insights regarding the power consumption of AMI equipment and the challenges involved with extending the schemes functionality to other energy domains. We have included additional discussion of the points you raise in order to address these areas of concern.

Author action: Updated the conclusion (Section 8):
Other metered utilities, such as water and gas, may also potentially benefit from our solution, although extending the scheme to these areas may present novel domain-specific challenges.

Reviewer #4

Concern #1
In the instruction, please summarize the main innovative points of this paper again, for example: The detailed contributions of this study are summarized as follows:1.Presents a xxx method, which can xxxxxxxxxxx. 2.xxxxxxxxxx. 3.xxxxxxxxxxxxxx.

Author response: Agreed. To emphasize this better, we added a clearer (and bolded) sentence in the introduction about key contributions. Wording was altered in a few places to improve communication of how the contributions impact operations. Finally, the list of contributions was enumerated, as recommended.

Author action: As stated above. The clearer sentence (new paragraph) is:
The **key contributions** of CHEA, introduced in this paper, include:

Concern #2
Suggest integrating the content of 2. Background and Motivation and 3. Related Work into one chapter, both of which are discussing the background.

Author response: The suggestion is appreciated, but we feel that there is enough of a conceptual difference between the two sections (domain concepts and problems in the background section, and current solutions in the related work section) to justify keeping them separate.

Author action: None.

Concern #3
Are Tables 2 and 3 three line tables? It is suggested to revise them carefully.

Author response: The tables do contain a header row and four content rows, each of which contain statistics for the four schemes being compared. The format has not changed, but the values in Table 5 (old Table 3) were updated for a more accurate assessment of the performance.

Author action: Table 5 (old Table 3) updated.

Concern #4
In this paper, the protocol was tested using a software simulation of a smart grid environment, What software is being used? How are the parameters set? Can you explain the effectiveness of the algorithm in this article?

Author response: The performance results have been updated to more clearly delineate between comparisons to other schemes versus demonstrating the effectiveness of the scheme

under various conditions. The software used is already available online (https://github.com/Smart-Contract-Modelling-uOttawa/CHEA-Simulation, reference [44]).

Author action: Updated Section 6 to better explain comparisons and created Section 6.3 for scheme analysis.

Concern #5

The transactive energy market is an emerging development in energy economics built on advanced metering infrastructure. Data generated in this context is often required for market operations, while also being privacy sensitive. Therefore, for this topic, data encryption algorithms are very important. Suggest the author to cite some of the latest relevant research literature. Such as:

[1] Kou, L.; Wu, J.; Zhang, F.; Ji, P.; Ke, W.; Wan, J.; Liu, H.; Li, Y.; Yuan, Q. Image encryption for Offshore wind power based on 2D-LCLM and Zhou Yi Eight Trigrams. International Journal of Bio-Inspired Computation. 2023, 22(1): 53-64. https://doi.org/10.1504/IJBIC.2023.133505

[2] O. M. Al-Hazaimeh, M. F. Al-Jamal, A. K. Alomari, M. J. Bawaneh, and N. Tahat, "Image encryption using anti-synchronisation and Bogdanov transformation map," International Journal of Computing Science and Mathematics, 2022, vol. 15, no. 1. pp. 43–59.https://doi.org/10.1504/IJCSM.2022.122144

[3] Cheng, Y.; Liu, Y.; Zhang, Z.; Li, Y. An Asymmetric Encryption-Based Key Distribution Method for Wireless Sensor Networks. Sensors 2023, 23, 6460. https://doi.org/10.3390/s23146460

Author response: We appreciate the reviewer's suggestions of relevant research. Papers 1 and 2 propose encryption schemes for the energy sector, which are notable but not directly applicable to the problem addressed by the proposed scheme (enabling privacy-preserving analysis of energy usage data). Paper 3 proposes a key distribution scheme that is now mentioned explicitly in the related work to contrast with the approach we propose (thanks for this reference!).

Author action: Updated related work:

Key distribution is a central problem for traditional schemes, such that it has become its own area of research. For example, Cheng et al. [38] propose a key distribution scheme that reduces communication overhead and improves security. One can thus conclude that avoiding key distribution altogether would be a valuable proposition.