Privacy-preserving Spectral Estimation in Smart Grid

Yue Tong, *Student Member, IEEE,* Jinyuan Sun, *Member, IEEE,* Kai Sun, *Member, IEEE*

***Abstract*—Inter-area Oscillations pose serious threats to the stability of power transmission grids. Failure to notice or to handle inter-area oscillations may lead to widespread catastrophic blackouts. It is, therefore, critically important to monitor the oscillation conditions such that timely mitigation controls can be applied at the early stage. Recent research shows that it is an effective approach to continuously track the frequency domain of ambient phasor measurement units (PMU) data for the monitoring purpose. However, since inter-area oscillations usually involve multiple utility companies, tracking them requires PMU data from some different trust domains, which raises data privacy concerns. To address these concerns, we proposed privacy-preserving multiparty spectral estimation, which enables power grid operators to obtain the power spectrum of PMU measurement data, while the data remain encrypted. A case study was also carried out, which showed that the proposed scheme is secure, efficient, and practical.**

***Index Terms*—security, data confidentiality, cloud computing, outsourcing, disguising technique, homomorphic encryption, secure computation**

I. Introduction

Inter-area oscillations are detrimental to the stability of the power transmission grids. Poorly damped oscillations reduce the capability of the power transfers and even lead to widespread blackouts. Incidents such as Western Interconnection Blackout on Aug. 10 (1996), US Blackout on Aug. 14 (2003), Italian Blackout on Sept. 28 (2003) have demonstrated the serious damages that inter-area oscillation can make. Therefore, in order to keep the lights on, it would be extremely helpful to continuously track the oscillation conditions and provide the control room with early warnings before a potential oscillation develop into a real catastrophic inter-area oscillation.

Recently, real-time measurement data collected by phasor measurement units (PMU) have been shown helpful to monitor and detect inter-area oscillations in the power system. As one of the key enabling technology for the smart grid, PMU technology makes real-time monitoring of power systems possible. The data collected by PMUs include time-stamped instant voltage, current, rotor angle, and frequency. PMU measurement data have been utilized to 1) support real-time grid operations, 2) improve system planning and analysis, and 3) provide response-based control applications [15]. When it comes to the study of power system's low-frequency oscillations, a host of research [17], [21], [7] apply frequency domain approaches to PMU measurement data, which examines the frequency domain of PMU measurements, and uses methods such as Frequency Domain Decomposition (FDD)[6], [5], computing risk scores[17], or tracking the oscillation modes[21].

For these frequency domain approaches, conducting spectral estimations is the starting point. To obtain spectral estimations, we note that existing frequency domain approaches all assume they have unrestricted access to all the measurement data of the ambient PMUs. Nonetheless, privacy concerns regarding the use of PMU measurement data exist in real practice. In the current deregulated power market, the transmission grid comprises competing utility companies running their own power systems under the coordination of independent system operator (ISO). The utility companies consider the PMU measurements taken at their own power system private and sensitive, as *North American Electricity Reliability Corporation Confidentiality Agreement for Electric System Operating Reliability Data*[8] points out that *"the operational reliability data may contain proprietary information and unequal access to operational reliability data may result in unfair advantages and disadvantages in the electricity market"*. In fact, according to [9], *"Since deregulation, a competitive environment has arisen and complete information about the state of the power grid is seldom available to operators"*. Although legal agreements like [8] exist to try to ensure the privacy of sensitive data while they are being used in research and operations, there are no technical guarantees. As a consequence, in spite of benefits, the lack of privacy protection seriously discourages utility companies from sharing their data.

Our contributions In this work, we take the first step to investigate privacy-preserving multiparty spectral estimations to demonstrate the feasibility of conducting spectral estimation without sacrificing data privacy. We address this open problem mainly leveraging the cloud computing and Paillier cryptosystem [16].

Our contribution is summarized as follows:

- To our best knowledge, for the first time, this work considers the privacy-preserving spectral estimation in the multiparty scenario.
- Software prototype of the proposed scheme is developed and tested. Additionally, taking into account the characteristics of discrete Fourier transform, optimizations are proposed to reduce the latency incurred by extra cryptographic computations, and, thus, making the proposed method more efficient and practical.

We organize the rest of this paper as follows. Section II reviews related works. Section III talks about the background knowledge. Section IV introduces settings and system model and formulates the problem we would like to solve. The

Yue Tong, Jinyuan Sun and Kai Sun are with the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37921 USA e-mail: {ytong3, jysun, ksun}@utk.edu

section continues to present the proposed scheme and relevant algorithms. Section V presents a case study of the proposed scheme with the simplified model of WECC AC transmission system and some practical optimizations to improve further the efficiency of the proposed scheme. We conclude this paper and talk about future works in Section VI.

II. Related works

Our work falls into the broad category of non-interactive privacy-preserving signal processing. Although, to our best knowledge, our scheme is the first to deal with privacy-preserving spectral estimations involving multiple parties, we have drawn significant inspiration from the previous research. The most closely related work is [2] by Bianchi *et al.* , which demonstrates the feasibility of carrying out Fourier transform in the encrypted domain. Lagendijk *et al.* [13] surveys existing privacy-preserving signal processing utilizing homomorphic encryption and secure multiparty computation. Both works above, however, deal with only the minimal scenario where a single party wishes to offload the computation to an untrusted processing device.

Our scheme aims at addressing utility companies' privacy concerns at the generation and transmission level of smart grid; previous research on privacy preservation in smart grid, however, mainly focus on the privacy of customer data. Shi *et al.* [10] proposes a scheme that enables privacy-preserving aggregation residential power consumption on a untrusted aggregator. This scheme only works for aggregation of encrypted data. Similar problems are also investigated regarding consumers' privacy protection in [4], [18], [1]. A very few existing works consider the data privacy problem of operational data in the bulk power system. Tong *et al.* presents a secure data sharing scheme for situational awareness for the power grid in [19]. It is, however, limited to secure data archiving and access control for the power flow data; furthermore the processing and manipulation of the shared data still need to be conducted in a fully trusted environment in [19].

III. Preliminaries

A. Fourier Transform

Fourier transform is a widely-used fundamental signal processing tool to obtain the spectral estimation of a signal. An M-point discrete Fourier transform (DFT) of a finite time-series signal $x(n)$ of length T is given by:

$$X(k) = \sum_{n=1}^{T} x(n) W^{nk}, k = 1, 2, ..., M$$

where $W = e^{-\frac{j2\pi}{M}}$. The $X(k)$ is a complex number that indicates the signal's magnitude and angle in the k-th frequency component. In the rest of the paper, unless otherwise stated, we assume $M = T$, which is a typical choice without loss of generality.

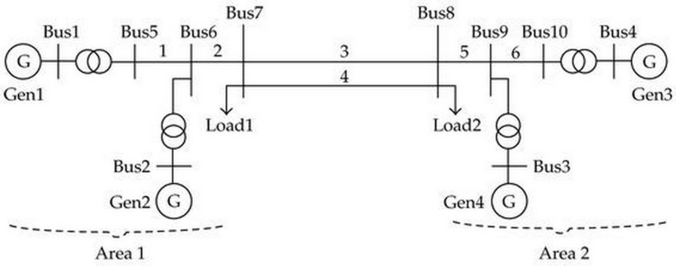

Fig. 1: Two area four generator power system from [12]

B. Paillier Cryptosystem

Paillier cryptosystem [16] is based on the decisional composite residuosity assumption. It is widely known as an additive homomorphic cryptography. It enables one to compute the encryption of the sum of two value, say $m_1 + m_2$, given only the encryptions of m_1 and m_2. We briefly revisit Paillier cryptosystem in this subsection.

Key Generation Let p and q be big prime numbers and $N = pq$, such that N is hard to factorize. Let the private key be the least common multiple of $(p-1, q-1)$, *i.e.*,$K_{priv} = lcm(p-1, q-1)$. Let $g \in \mathbb{Z}^*_{N^2}$ an element of order αN for some $\alpha \neq 0$. The public key is the tuple (N, g).

Encryption To encrypt a value m, where $m < N$, generate a random value $r < N$, and use the public key to encrypt the value. The ciphertext is constructed as: $c = Enc(K_{pub}, m) = g^m r^N \mod N^2$.

Decryption Given the ciphertext ct, one can decrypt for the plaintext with the private key, as

$$m = Dec(K_{priv}, ct) = \frac{L(c^{K_{priv}} \mod N^2)}{L(g^{K_{priv}} \mod N^2)} \mod N$$

where $L(x) = \frac{x-1}{N}$.

Additive homomorphism Given the ciphertext of m_1 and m_2, which are $g^{m_1} r_1^N$ and $g^{m_2} r_2^N$, respectively, one can compute the ciphertext of $m_1 + m_2$.

$$\begin{aligned} Enc(K_{pub}, m_1) Enc(K_{pub}, m_2) &= g^{m_1+m_2}(r_1 r_2)^N \\ &= Enc(K_{pub}, (m_1 + m_2)) \quad (1) \end{aligned}$$

$Enc(K_{pub}, m_1 + m_2)$ can be decrypted with the same private key that is used to encrypt m_1 and m_2.

Homomorphic multiplication of plaintext Given the ciphertext $g^m r^N$, one can also calculate the ciphertext of θm, where θ is a constant number, by computing

$$(g^m r^N)^\theta = g^{\beta m}(r^\theta)^N = Enc(K_{pub}, \theta m)$$

C. Monitoring Oscillation in power system

Figure 1 depicts the classical two area power system introduced in [12] with two generators in each area. Inter-area oscillations may develop at the interface 12-34. That is between the generator cluster $C1$, consisting of generators $G1$ and $G2$, and the generator cluster $C2$, consisting of generators $G3$ and $G4$. PMUs installed at the respective generators monitor the generators' rotor angles. Then, potential oscillations can be

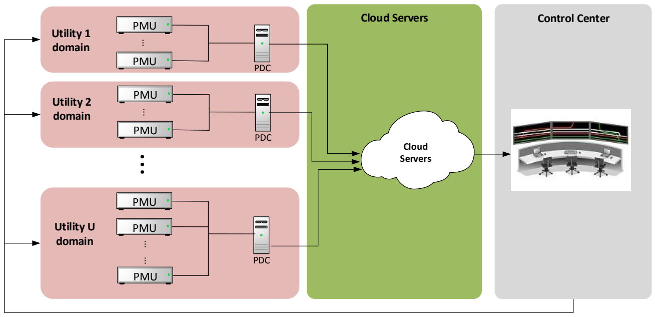

Fig. 2: System Model of privacy-preserving processing of PMU data

monitored and analyzed by continuous tracking the spectra of the averaged angles of the two areas.

We denote the time series of rotor angles of the four generator as δ_1, δ_2, δ_3, and δ_4, respectively. The angle of Area 1 is represented by the averaged rotor angle of the two generators in the area, *i.e.* $\delta_I = \frac{1}{2}(\delta_1+\delta_2)$. Similarly, the angle of Area 2 is given by $\delta_{II} = \frac{1}{2}(\delta_3 + \delta_4)$. Thereby, what we would like to monitor is the spectrum of $\tilde{\delta}_I$ and $\tilde{\delta}_{II}$, where $\tilde{\delta} = \delta - mean(\delta)$ denote the mean centering δ.

IV. Our proposed scheme

A. Problem formulation

1) System model and entities: The system model of the proposed scheme is captured in Fig. 2. Each participating utility has several PMUs reporting their real-time measurements of rotor angles to the cloud servers. Since the PMU measurement data must be protected against unauthorized access of peer utility companies, cloud servers, and the control room, each PMU sends to the cloud servers the measurement data in their encrypted form. Next, the cloud servers receive the encrypted measurements and perform relevant computations to securely obtain the encrypted spectral estimation without knowing the real values of the input data. The cloud then forwards the encrypted spectrum to the control room. Finally, the operator at the control room receives and decrypts the spectrum. There also exists secure communication channels between utility companies and the control room for key assignments and other communications.

We justify the introduction of the public cloud with following arguments. First, it has been observed a remarkable trend for the power industry to take advantage of cloud computing to cope with the soaring volumes of data generated and the responding rapidly growing demand for computing capability. Using the service of Cloudera, the cloud computing company, TVA began to manage the large volume of data collected from 103 PMUs (as of 2009), for better reliability and scalability [3]. Additionally, ISO New England started to explore leveraging cloud computing to conduct dynamic simulations not only faster but also less expensive [11], [14]. Second, the cloud has abundant computational resources so that it can handle the substantial computation incurred by the cryptographic operations in the privacy-preserving scheme within an acceptable latency. Finally, by letting the control room hold only the decryption key, but not the encrypted measurement data, which is only accessible to the cloud, the system model prevents the control room from abusing the privilege of decryption.

2) Trust model and security goals: In the above system model, the public cloud servers are modeled as semi-honest. It means that the cloud is legally obligated to strictly follow the pre-defined protocol specifications and to correctly conduct the computation, but it will inevitably look at the information sent in and out.

Our scheme also assumes that the cloud and the control room does not collude with each other.

With the above assumption, the security goal of our system is two-fold:

1. to ensure none of the data sent by individual utilities will be disclosed to any parties other than the data owner itself.
2. only the spectrum will be disclosed to the control room.

B. Monitoring inter-area oscillations

Our proposed scheme adopts the framework of [17] and consists of two phases, namely, *offline analysis* and *online monitoring*.

The offline analysis is similar to that of [17]. This stage aims at simplifying the power system model by aggregating generators into clusters that may oscillate against each other. The aggregation can be done with generator coherency identification methods such as 1) Tolerance base method and 2) Weak Links Based Method, according to [17]. The offline analysis does not require sensitive real-time measurements and, thus, can be conducted beforehand without privacy concerns.

The online monitoring phase estimates the spectrum of each cluster's angle. To this end, it is assumed that each cluster has several PMUs installed to monitor the rotor angles of the generators in the cluster. A cluster's angle is given by the average of the angles reported by PMUs belonging to that cluster.

To be more specific, we use δ_{C1} through δ_{CK} to denote the averaged rotor angles of Custer 1 through K; we also use δ_{Cki} to denote the rotor angles reported by the i-th PMU in the k-th cluster. Thus, $\delta_{Ck} = \frac{1}{|Ck|}\sum_{i=1}^{|Ck|}\delta_{Cki}$, where $|Ck|$ is the number of PMUs in Cluster k. Without having any security considerations, the control room can get the spectral estimation of the angle of cluster k at time t, denoted by $F_{\delta_{Ck}}(k_\omega)$, for $k_\omega = 0, 1, 2, ..., N$. by the following procedures. 1) first have all the PMUs in the k report their measurements of rotor angles denoted by δ_{Cki} for $\{i = 1, 2, ..., |Ck|\}$, 2) compute the clusters' angle as $\delta_{Ck} = \frac{1}{|Ck|}\sum_{i=1}^{|Ck|}\delta_{Cki}$, 3) apply Fourier transform to the mean centering cluster angle $\tilde{\delta}_{Ck} = \delta_{Ck} - \langle\delta_{Ck}\rangle$, where $\langle\delta_{Ck}\rangle$ is the iterative mean of δ_{Ck}. $\langle\delta_{Ck}\rangle$ is updated as $\langle\delta_{Ck}(t)\rangle = \frac{t}{t+1}\langle\delta_{Ck}(t-1)\rangle + \frac{1}{t+1}\delta_{Ck}(t)$, as the time advances.

In what follows, we present the proposed privacy-preserving multiparty spectral estimation that allows for secure calculation of $F_{\delta_{Ck}}(k_\omega)$ without the knowing real values of δ_{Cki}.

C. Privacy preserving multiparty spectral estimation

The basic idea is to secure each procedure of the above non-privacy-preserving approach using the homomorphic encryption.

Setup Once the online monitoring is activated, all the concerned parties make agreements on T, the length of the time window and, N, the number of points of the DFT ($T = N$ assumed), f_{PMU}, PMU's sampling rate, f_{spec}, the frequency to conduct spectral estimation. Upon successful agreement, the control room is notified to invoke procedures of cloud-assisted multiparty privacy-preserving spectral estimation.

Key generation The operator at the control room initializes the Paillier cryptosystem as described in Section III-B. The operator keeps the private key to itself and assigns the public key to the cloud as well as all the participating utilities. In reality, a utility may have more than one PMUs contributing. However, for ease of presentation, we assume that each utility have only one PMU taking part in the multiparty spectral estimation.

Uploading encrypted input For every $\frac{1}{f_{spec}}$ second, each PMU encrypts their new measurement data using the public key. For example, the i-th utility in the Cluster k encrypts its measurements $\delta_{\mathbf{Cki}}$ as $E(\delta_{\mathbf{Cki}}) = \{E(\delta_{Cki}(t)\}$ for $i = 0, 1, 2, ..., T-1$, where $E(\cdot)$ is a shorthand of $E(K_{pub}, \cdot)$ hereafter, if there is no confusion.

Privacy preserving spectral estimation Now using the data received from PMUs, the cloud securely estimates the latest spectrum by applying privacy-preserving Fourier transform to the data of the most recent time window for each cluster. Algorithm 1 details the privacy-preserving Fourier transform. The algorithm first securely derives the averaged angle of a cluster in the time window. It then securely calculates the corresponding iterative mean of the cluster's angle and mean centering cluster angle. Finally, the algorithm applies privacy-preserving discrete Fourier transform to the mean centering cluster angle gives the encrypted spectral estimation. Algorithm 1. calls supporting a sub-algorithm Algorithm 2. Since all computations are carried out in the encrypted domain, none of the measurement data is leaked to the cloud.

Result decryption The control room receives encrypted frequency coefficients as a result of Algorithm 1 from the cloud. It then decrypts for the frequency coefficients using decryption method of Paillier cryptosystem with the private key. Upon decrypting all coefficients, the control room obtains the spectral estimation of the PMU measurement data over the latest time window. The spectral estimation is then used for visualization, monitoring, or other frequency domain approaches.

In this paper, we mainly considered the magnitude of the power spectrum and developed practical privacy-preserving Fourier transform for PMU measurement data accordingly. The mode shape that is needed for determining oscillation boundaries could also be protected by applying homomorphic encryption to the angle of the cross-spectral density (CSD) given in [20]. However, it is not straightforward to extend our scheme to include damping where Prony's method should be applied, which we leave as our future work.

Algorithm 1: Privacy-preserving spectral estimation of a generator cluster's angle

```
Data: $E(\delta_{Cki})$, $E(r_i(k_\omega))$ for $i = 1, 2, ..., |Ck|$,
      $t = 0, 1, 2, ..., T-1$, $k_\omega \in \{0, 1, 2, ..., N-1\}$;
        $T$ Length of the time window, $N = T$ ;
        $|Ck|$ Number of generator in the cluster;
Result: Encrypted frequency coefficients $EncSpectrum$
Initialize EncSpectrum an zero-initialized vector of length $N$;
/* Homomorphically compute the averaged rotor angle of cluster $k$ */
for $t = 0$ to $T-1$ do
    $E(\sum_{i=1}^{|Ck|} \delta_{Cki}(t)) = \prod_{i=1}^{|Ck|} E(\delta_{Cki}(t))$;
    $E(\delta_{Ck}(t)) = E(\frac{1}{|Ck|} * \sum_{i=1}^{Ck} \delta_{Cki}(t))$
end
/* Obtain the mean centering cluster angles */
for $t = 0$ to $T-1$ do
    /* Calculate the iterative means of $\delta_{Ck}$ within the past second. Note that $\frac{t}{t+1}$ and $\frac{1}{t+1}$ are constant and can be multiplied with ciphertexts */
    $E(\langle\delta_{Ck}(t)\rangle) = E(\frac{t}{t+1}\langle\delta_{Ck}(t-1)\rangle + \frac{1}{t+1}\delta_{Ck}(t))$ ;
    /* using homomorphic addtion by Paillier cryptosystem and Algorithm 2 */
    /* Get cluster mean $\delta_{Ck}$ */
    $E(\tilde{\delta}_{Ck}(t)) = E(\delta_{Ck}(t) - \langle\delta_{Ck}(t)\rangle)$ ;
    /* Homomorphic subtraction by Paillier cryptosystem */
end
/* Securely apply $N$-point DFT to $\tilde{\delta}_{Ck}$ */
for $k_\omega = 0$ to $N-1$ do
    for $t = 0$ to $T-1$ do
        /* Calculate the respective element in the DFT matrix */
        $W_{tk_\omega} = W^{tk_\omega} = e^{-\frac{j2k_\omega t\pi}{M}}$;
        Securely calculate $E(\tilde{\delta}_{Ck}(t) * W_{tk_\omega})$ ;
        /* using Algorithm 2 */
        /* Securely accumulate the result to EncSpectrum$[k_\omega]$ */
        EncSpectrum$[k_\omega]$ =
        EncSpectrum$[k_\omega] \cdot E(\tilde{\delta}_{Ck}(t) * W_{tk_\omega})$
    end
end
return EncSpectrum
```

Algorithm 2: Multiply a encrypted complex number with a constant complex number

```
**Data**: An encrypted complex number $(E(a), E(b))$;
An constant complex number $c + di$;
**Result**: Encryption of the complex number
        $(a + bi)(b + ci)$
$encProd_R = E(a)^b(E(b)^c)^{-1} \mod N^2)$ ;      /* get the real part */
$encProd_I = E(a)^c(E(b)^d \mod N^2)$ ;   /* get the imaginary part */
**return** $(encProd_R, encProd_I)$
```

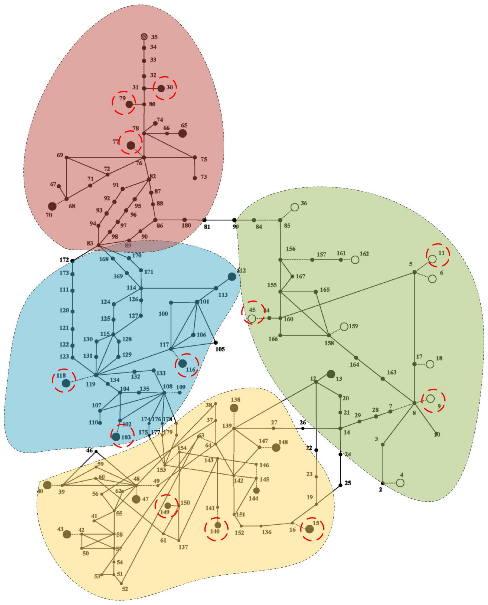

Fig. 3: Coherent generator clusters in WECC 179 bus system

V. A case study with WECC 179 bus system

We fully implemented the scheme with Java's BigInteger library. We used the key length of 512 bits to initialize the Paillier cryptosystem. All experiments are conducted on Linux servers with 8-core Intel Core i7 processor and 16GB RAM.

We tested the proposed scheme with a simplified model of the WECC AC transmission system with 29 generators and 179 buses[17]. As illustrated in Figure 3, offline analysis indicated that generators in the transmission grid were split into four coherent clusters. Each cluster was monitored by three PMUs, which are circled in the figure. A cluster angle was obtained by averaging the rotor angles measured by the three PMU in the respective cluster. The sampling rates of the PMUs were 100 Hz. Every second, privacy-preserving spectral estimation was conducted to update the power spectrum of cluster angles over the latest 40 second window (containing 4,000 measurements), with a 39-second overlap with the last time window.

For the demonstration purpose, four successive three-phase faults were simulated at 40s, 80s, 120s, and 160s, respectively, at a dynamic simulation. All PMU measurement data were obtained through the dynamic simulation and later used in the case study.

Following optimizations were applied to speed up the processing.

1 Compute only the frequency coefficients (4th through 40th) corresponding to the $[0.1, 1]$ Hz, which is the frequency range the inter-area oscillations may develop at.
2 As frequency coefficients in a discrete Fourier transform can be calculated independently, the computation were parallelized with 12 servers in the same computer cluster. Each handles three coefficients.
3 Precompute the DFT matrix and build an in-memory lookup table before runtime for each server.

With these optimizations, the average latency to obtain the spectral estimation of a single time window (40s) worth of measurement data was 0.95 second, which was less than the period of conducting spectral estimations (1 second).

The encrypted and decrypted spectral estimations over the simulated time were visualized using spectrograms in Figure 4 and Figure 5, respectively. As seen in the encrypted spectrograms, which was obtained by directly visualizing the result of Algorithm 1, the visualization was completely randomized, and no pattern could be observed. In the decrypted version, the visualization showed that frequency responses emerged and died down as the faults were applied and cleared. Obvious oscillation modes are seen around 0.2Hz, 0.5Hz, and 0.75 Hz, with the 0.2 Hz mode being the dominant one. The results of spectral estimations were also in accordance with the result of the small-signal analysis. The obtained spectral estimations could also be used for further research and analysis, which is, however, beyond the scope of this paper.

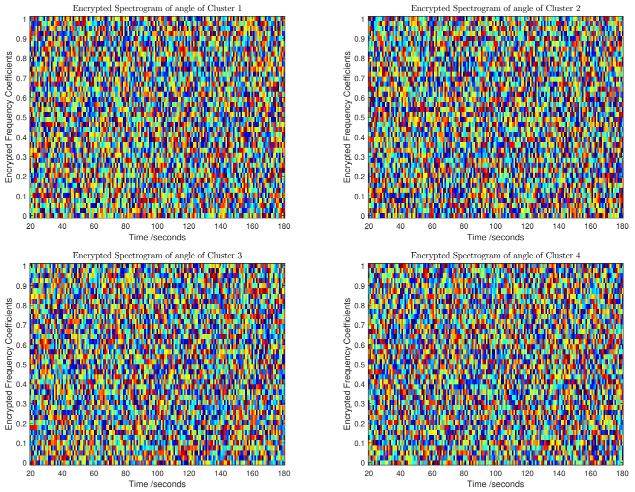

Fig. 4: Encrypted spectrograms of clusters' angles

VI. Conclusions

In this work, we presented a cloud-assisted multiparty spectral estimation for inter-area oscillation monitoring. The proposed scheme leverages the homomorphic Paillier cryptosystem to enable computations directly over the encrypted PMU measurement data. It was shown that the proposed scheme

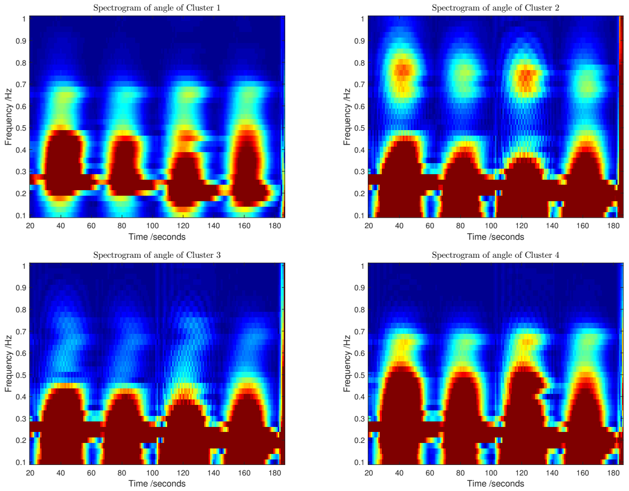

Fig. 5: Decrypted spectrograms of clusters' angles

can effectively protect the privacy of the PMU measurement data while generating desired spectral estimations. In future works, we will investigate methods to achieve auditability, by, for example, enabling the control room to validate the cloud server's work with zero knowledge proof, so we can relax the assumption that the cloud servers must be semi-honest. Another research direction worth exploring is to extend the idea of using the homomorphic encryptions to the Prony's method, which is more commonly used in the analysis and research of low-frequency oscillation in the power system.

Acknowledgment

This work was partially supported by the NSF/DoE Engineering Research Center (ERC) under NSF Award EEC-1041877. In addition, this work was partially supported by NSF under grant CNS-1422665.

References

[1] Z. Baharlouei and M. Hashemi. Efficiency-fairness trade-off in privacy-preserving autonomous demand side management. *Smart Grid, IEEE Transactions on*, 5(2):799–808, March 2014.

[2] T. Bianchi, A. Piva, and M. Barni. On the implementation of the discrete fourier transform in the encrypted domain. *Information Forensics and Security, IEEE Transactions on*, 4(1):86–97, March 2009.

[3] Christophe Bisciglia. The smart grid: Hadoop at the tennessee valley authority (tva). http://blog.cloudera.com/blog/2009/06/smart-grid-hadoop-tennessee-valley-authority-tva/, 2009. Accessed: 2014-09-28.

[4] Fabio Borges, Denise Demirel, Leon Bock, Johannes Buchmann, and Max Muhlhauser. A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing. In *Computers and Communication (ISCC), 2014 IEEE Symposium on*, pages 1–6, June 2014.

[5] Rune Brincker, C Ventura, and Palle Andersen. Damping estimation by frequency domain decomposition. *IMAC XIX, Kissimmee, USA*, 2001.

[6] Rune Brincker, Lingmi Zhang, and P Andersen. Modal identification from ambient responses using frequency domain decomposition. In *Proc. of the 18*International Modal Analysis Conference (IMAC), San Antonio, Texas*, 2000.

[7] S. Chakrabarti, E. Kyriakides, Tianshu Bi, Deyu Cai, and V. Terzija. Measurements get together. *Power and Energy Magazine, IEEE*, 7(1):41–49, January 2009.

[8] North American Electric Reliability Corperation. Operating reliability data confidentiality agreement, version 3. http://www.nerc.com/comm/OC/Pages/ OperatingReliability DataConfidentialityAgreement.aspx, 2009. Retrieval date: Nov. 20th, 2014.

[9] PNNL EIOC. Situational awareness. url: http://eioc.pnnl.gov/research/sitawareness.stm, 2013. accessed Oct 8, 2014.

[10] Richard Chow Elaine Shi, T h. Hubert Chan, Dawn Song, and Eleanor Rieffel. Privacy-preserving aggregation of time-series data. In *In NDSS*, 2011.

[11] ISO New England. Regional electricity outlook, 2014.

[12] Prabha Kundur, Neal J Balu, and Mark G Lauby. *Power system stability and control*, volume 7. McGraw-hill New York, 1994.

[13] R.L. Lagendijk, Z. Erkin, and M. Barni. Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation. *Signal Processing Magazine, IEEE*, 30(1):82–105, Jan 2013.

[14] Eugene Litvinov. Early experience with cloud computing at iso new england, 2014.

[15] North America Electric Reliability Corporation, NERC. Real-time application of synchrophasors for improving reliability. http://www.nerc.com/docs/oc/rapirtf/RAPIR retrieval data: 10/12/2014.

[16] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in cryptologyEUROCRYPT99*, pages 223–238. Springer, 1999.

[17] Kai Sun, Xiaochuan Luo, and J.M. Wong. Early warning of wide-area angular stability problems using synchrophasors. In *Power and Energy Society General Meeting, 2012 IEEE*, pages 1–6, July 2012.

[18] C. Thoma, Tao Cui, and F. Franchetti. Privacy preserving smart metering system based retail level electricity market. In *Power and Energy Society General Meeting (PES), 2013 IEEE*, pages 1–5, July 2013.

[19] Yue Tong, J. Deyton, Jinyuan Sun, and Fangxing Li. s^3a : A secure data sharing mechanism for situational awareness in the power grid. *Smart Grid, IEEE Transactions on*, 4(4):1751–1759, Dec 2013.

[20] D.J. Trudnowski. Estimating electromechanical mode shape from synchrophasor measurements. *Power Systems, IEEE Transactions on*, 23(3):1188–1195, Aug 2008.

[21] L. Vanfretti, S. Bengtsson, V.S. Peric, and J.O. Gjerde. Spectral estimation of low-frequency oscillations in the nordic grid using ambient synchrophasor data under the presence of forced oscillations. In *PowerTech (POWERTECH), 2013 IEEE Grenoble*, pages 1–6, June 2013.