Power Analysis Side-Channel Attacks on Same and Cross-Device Settings: A Survey of Machine Learning Techniques

Ashutosh Ghimire, Vishnu Vardhan Baligodugula, and Fathi Amsaad(✉)

Wright State University, Dayton, OH 45435, USA
{ghimire.18,baligodugula.2,fathi.amsaad}@wright.edu

Abstract. Systems that use secret keys or personal details are seriously at risk from side-channel attacks, especially if they rely on power analysis. Attackers can use unintentional sources like power consumption and electromagnetic waves to extract sensitive information. Recently, machine learning has become a promising approach for executing power side-channel attacks that are efficient and effective for single and cross-device environments. This paper reviews various machine learning-based power side-channel attacks, including feature extraction techniques, classification methods, and countermeasures. This survey investigates same-device and cross-device attacks that use multiple devices for training an artificial intelligence model for this purpose. It examines the strengths and limitations of various machine learning algorithms and suggests areas for future research to address challenges.

Keywords: Security · Artificial Intelligence · Attack · Power Traces · Cross-device

1 Introduction

The burgeoning of connected devices and the IOT ecosystem has resulted in an enormous increase in the amount of data created by these devices [13]. Unfortunately, this expansion has also presented attackers with new chances to exploit system weaknesses. Power side-channel attacks, for example, have arisen as a significant concern to the security of these devices. These attacks take advantage of unintended information leakage from a device, allowing an attacker to infer sensitive information about its operation by measuring its power consumption.

Power side-channel attacks can be particularly devastating because they can be performed remotely and without physical access to the target device. Moreover, traditional countermeasures, such as hardware or software-based protections, can be costly, impractical, or ineffective against these attacks. To address these challenges, researchers have turned to machine learning techniques to detect and prevent power side-channel attacks [15].

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 357–367, 2024.
https://doi.org/10.1007/978-3-031-45882-8_24

This paper aims to present a comprehensive survey of side-channel attacks built on machine learning, covering single and cross-device settings. Our analysis includes a detailed examination for the present situation-of-the-art in attack models, feature extraction, classification, and countermeasures. Our primary focus is on the challenges posed by cross-device attacks, where a single machine learning model is trained using data from multiple devices. We provide a critical review of the advantages and disadvantages of various machine learning approaches for side-channel attacks and identify possible paths for future studies to address the current challenges. Our goal is to create a valuable resource for researchers, practitioners, and policymakers interested in enhancing the security of connected devices (Fig. 1).

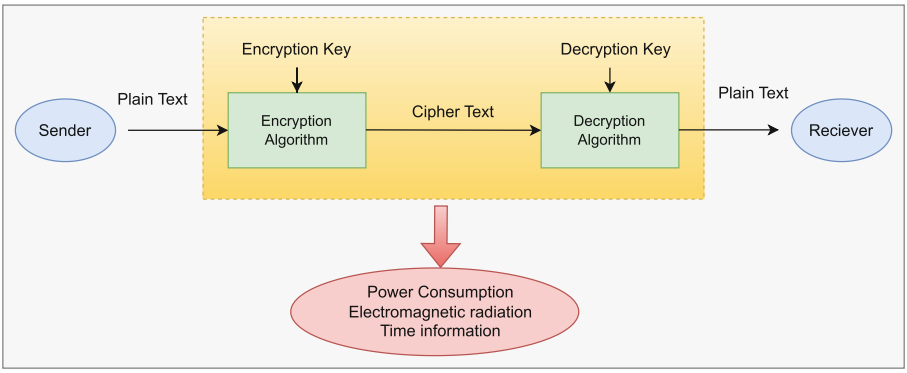

Fig. 1. Cryptosystems side channel information leakage

2 Background

2.1 Side-Channel Analysis (SCA)

Analyzing from the Side-Channel refers to various attacks that exploit unintended information leakage from a system's physical or implementation characteristics, such as electromagnetic radiation, timing information and power consumption. Such attacks can allow an attacker to obtain sensitive information about cryptographic keys or other secrets used within the system. Side-channel attacks can be categorized be determined by the type of side-channel signal used, including power analysis, electromagnetic analysis, acoustic analysis, and timing analysis.

Power Analysis (PA) is a sort of attack using side-channel information that analyzes the power usage of cryptographic equipment which can be divided into Differential Power Analysis (DPA) and Simple Power Analysis (SPA) [14]. Simple Power Analysis uses statistical analysis to directly examine the power usage of

the devices in order to derive the secret key. This strategy needs a vast collection of data. In contrast, Differential Power Analysis compares power traces from different inputs to identify statistical differences that reveal the secret key. DPA is more advanced than SPA, but it also requires more expertise and complexity in analysis. It is crucial to understand the differences between these two techniques to effectively counteract power analysis attacks.

2.2 Machine Learning

An area in artificial intelligence called machine learning works on creating models capable of learning from data and making decisions or predictions without explicit programming. Several domains, including natural language processing, speech recognition, picture identification, and anomaly detection, have adopted this strategy [2,4].

In the realm of power side-channel attacks, researchers have proposed machine learning methods to increase the precision and effectiveness of attack detection and key recovery. These techniques can be categorized according to the type of learning algorithm used, such as supervised, unsupervised, and reinforcement learning.

2.3 Cross-Device Settings

Power side-channel attacks in cross-device settings refer to attacks that exploit side-channel information leaked by a device to extract the secret key used by another gadget in a different setting. This can happen when the same cryptographic key is used across multiple devices or when the side-channel information leaked by one device can be used to infer information about the key used by another device.

Cross-device attacks can be more challenging than attacks on a same-device because they involve dealing with different settings and conditions, such as different device architectures, operating systems, and environmental factors. Therefore, machine learning techniques that can handle cross-device variations and generalize well across different settings are particularly useful in this context.

3 Literature Review

Recent years have witnessed increasing interest in developing methods over side-channel attacks relying on machine learning and cross-device settings. Various survey papers have been published, outlining the latest state-of-the-art techniques in this field, and it is crucial to review and analyze their contributions.

In their survey paper published in 2019, Lee et al. provided an extensive review of the latest deep learning approaches utilized in side-channel attacks (SCA), which included CNNs and RNNs, and examined their strengths and limitations [11]. Additionally, they underscored the significance of further research

and development in deep learning-based SCA techniques, particularly for their practical implementation.

Xu et al. (2021) proposed a method for cross-device attacks using unsupervised domain adaptation, which adapts the side-channel features extracted from a source device to a target device without requiring any labeled data from the target device [1]. The proposed technique shows significant improvement in attack performance compared to other existing methods.

Al-Ahmad et al. (2021) conducted a thorough review of power side-channel attacks, including their classifications, and the countermeasures designed to prevent them [16]. In their paper, the authors also discussed the challenges that hinder the progress of effective counter measures in case of these attacks.

In a separate study, Liu et al. (2021) proposed a novel method for stealing machine learning model parameters by taking advantage of the power consumption during model inference [21]. The proposed attack approach is capable of extracting sensitive information, such as the model weights and biases, which can be exploited to replicate the machine learning model and conduct further attacks.

This survey paper specifically focuses on cross-device settings for power side-channel attacks and explores the latent of artificial intelligence techniques in this area. We analyze the advantages and limitations of existing research and discuss the future directions of this field. Our paper aims to provide a more comprehensive understanding of the challenges and opportunities in cross-device power analysis side channel machine learning attack. It can serve as a useful reference for researchers and practitioners interested in understanding the latest developments and future directions in this field.

4 Machine Learning Approaches for Side Channel Analysis

SCA aim to obtain confidential information by exploiting the physical characteristics of a system, such as electromagnetic radiation or power consumption. In recent years, machine learning techniques have become a potent tool for improving the efficiency and efficacy of these assaults. This section will explore the latest advancements in machine learning based approaches for side-channel attacks, with a particular focus on two distinct settings: the same-device setting and the cross-device setting.

4.1 Same Device Setting

In the same-device setting, an attacker can obtain access to a same-device and monitor its side-channel emissions to extract confidential information. Recent advances in machine learning techniques have demonstrated encouraging outcomes in enhancing the efficiency and efficacy of side-channel attacks in this setting.

Convolution Neural Network. The use of Convolutional neural networks (CNNs) have gained increasing popularity in side-channel analysis to identify patterns in side-channel traces. Numerous studies have examined the potential of CNNs in exploiting information leakage from physical implementations of cryptographic systems such as AES, DES, and SHA. For instance, the paper [18] proposed a deep learning-based SCA approach using a CNN model for AES-128 with a single power consumption trace. Similarly, [12] suggested a 2D deep learning architecture for exploiting side-channel leakage in lattice-based key-exchange, whereas [24] introduced a multilabel deep learning-based SCA technique using a CNN model for AES-128 with a single power trace. These studies highlight the potential of CNNs in SCA for same-device settings and provide valuable perceptions by means of deep learning method in SCA.

LSTM. A study proposes a novel side-channel attack technique that uses a deep learning architecture cleaning-based STM and fully connected layers to predict secret key bits of an FPGA-based AES implementation [20]. The proposed attack technique is evaluated using two different types of attacks, SPA and DPA, and achieves a high success rate of 91.84% and 91.39%, respectively, outperforming existing side-channel attacks. The study uses power traces collected from an FPGA-based AES implementation, and the threat model assumes an attacker with access to these power traces.

DNNs. DNNs are widely used in side-channel analysis to extract sensitive information from cryptographic implementations. A novel side-channel attack technique is proposed in [10] that involves decomposing power traces into a linear combination of basis functions and subsequently using a DNN architecture to predict the secret key bits. The proposed method achieves high accuracy in predicting secret key bits and outperforms existing SCAs on AES and PRESENT implementations. The study uses power traces collected from cryptographic implementations, and the threat model assumes an attacker with access to these power traces.

Federated Learning. A federated learning-based side-channel attack technique is suggest in [19] to extract secret keys from devices while maintaining data privacy. The method involves training models on local datasets and aggregating the models' parameters on a server without disclosing any local information. The authors evaluate their approach on a smart card and demonstrate the effectiveness of the federated learning approach in extracting secret keys with improved accuracy while ensuring data privacy.

SVM. Support Vector Machines (SVMs) have gained popularity in side-channel analysis as a machine learning technique. In a recent study, the authors proposed a new attack method that utilizes SVMs to extract secret keys from cryptographic devices by analyzing the power consumption [7]. Their method involves

training SVMs on power traces and using them to classify the power consumption patterns associated with different secret key values. Authors successfully demonstrated the vulnerability of cryptographic devices by precisely extracting the secret key from a smart card implementation of the AES cipher.

4.2 Cross-Device Setting

In the cross-device setting, the attacker has access to multiple devices and can use side-channel information from one device to attack another device with a similar implementation. Recent machine learning techniques have shown promise in improving the effectiveness of cross-device SCAs.

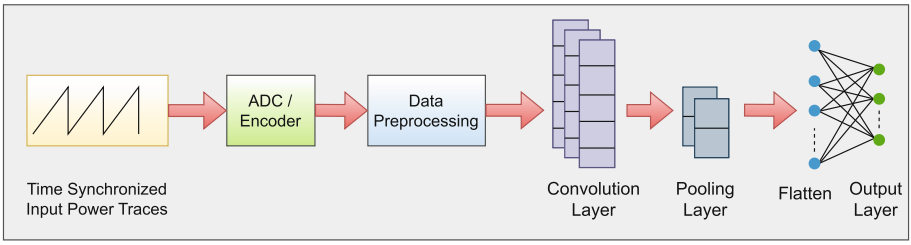

Fig. 2. Generic CNN training process for evaluating attack efficiency using power trace analysis.

CNN. CNNs are widely used in SCA to identify patterns in side-channel traces by capturing spatial dependencies between measurements. They have been applied to exploit information leakage from physical implementations of cryptographic systems, such as AES, DES, and SHA. Recent advances in deep learning-based SCA have been discussed in [3], along with their advantages and limitations. Another recent paper [9] proposes a CNN-based architecture using cross-subkey leakage that outperforms other methods on a new dataset. Figure 2 shows the generic example of training the CNN to assess the attack's effectiveness. The paper highlights the importance of considering cross-subkey leakage in side-channel analysis and provides a new avenue for developing deep learning-based techniques for practical implementation.

Autoencoder. Autoencoders are used in side-channel analysis as an unsupervised deep learning technique. In [5], The authors suggest a cross-device power side-channel attack using autoencoders. Their autoencoder-based attack model outperforms traditional methods in terms of success rate and accuracy, and they emphasize the importance of practical considerations such as low-cost sensors and real-time performance. In [23], the authors propose a denoising method called Noise2Clean using an unsupervised deep learning approach based on

autoencoders. The proposed method is effective in denoising side-channel traces without using any prior knowledge of the noise model. The authors compare their results with other denoising methods and show that their method outperforms them in terms of denoising performance on two different datasets.

Transfer Learning. Transfer learning has become a popular technique in deep learning-based side-channel analysis, where pre-trained models on large datasets are leveraged to improve performance on smaller datasets. For instance, a study proposed a cross-device profiled SCA adapting pre-trained models for different devices utilizing the meta-transfer learning, and achieving better performance with fewer samples [22]. The authors evaluated their method on datasets including AES, DES, and SHA-3. Authors demonstrated an advanced side-channel attack using transfer learning and deep learning-based cross-family profiling that outperforms traditional and other deep learning-based methods [17]. They evaluated their method on datasets including AES and PRESENT and suggested that it enhances the transferability of deep learning-based SCA techniques across different cryptographic algorithms.

PCA. In SCA, feature analysis method like Principle Component Analysis is a widely used for reducing the dimensionality of data. Recently, researchers conducted a study where they successfully applied PCA to perform a side-channel attack on a software performance of AES-128. The study described the trial design and outcomes, emphasizing how the use of PCA significantly improved the attack success rate by reducing the dimensionality of power traces [8]. However, the paper also acknowledged the limitations of PCA and recommended exploring alternative dimensionality reduction techniques for side-channel analysis. Overall, this research highlights the potential of PCA in side-channel attacks and encourages further investigation into other methods to enhance the security of cryptographic implementations.

Support Vector Machine and Random Forest Classifier. SVM and random forest are two popular machine learning approaches in the area of side-channel analysis. A current study [6] investigates the suitability of these algorithms for multi-device profiling side-channel attacks, taking into account factors such as No of profiling traces, number of gadgets in the training set, and type of leakage model. The findings suggest that random forest performs better than SVM, especially when the number of profiling traces is small. This research provides valuable insights from the effectiveness of machine learning approaches to multi-device profiling side-channel attacks, aiding the selection of appropriate algorithms for such scenarios.

5 Strength and Limitations

In recent years, machine learning techniques have shown increased accuracy and efficiency in power side-channel attacks across different devices and architec-

Table 1. Table showing summary of the techniques

Machine Learning Approach	Strengths	Limitations	Paper/s
CNN	Able to learn complex features from raw power traces; good performance in cross-device and same-device scenarios	Requires large amounts of data and computational resources; vulnerable to overfitting	[3,9,12,18,24]
Autoencoder	Able to extract useful features and denoise power traces; practical and efficient for cross-device attacks	Limited to simple attack scenarios; requires manual selection of hyperparameters	[5,23]
Transfer Learning	Effective for transferring knowledge between different devices and attack scenarios; reduces the amount of required training data	Limited to similar devices or attacks; requires careful selection of transfer learning strategy	[17,22]
PCA	Simple and efficient; effective in same-device attacks	Limited to simple attack scenarios and linear correlations	[8]
SVM and Random Forest	Effective in multi-device profiling attacks; computationally efficient	Limited to linear correlations and simple attack scenarios	[6,7]
LSTM	Able to capture temporal dependencies in power traces; effective in same-device attacks	Requires careful tuning of hyperparameters; limited to simple attack scenarios	[20]
DNN	Able to simulate intricate non-linear connections between power traces and secret keys; effective in multi-device attacks	Requires large amounts of data and computational resources; vulnerable to overfitting	[10]
Federated Learning	Protects privacy of individual devices; reduces communication overhead	Limited to similar devices and attacks; requires careful selection of aggregation strategy	[19]

tures, making them a versatile tool in this field. However, limitations such as the requirement for large amounts of training data and the variability of targeted devices can limit their effectiveness. Despite these challenges, machine learning approaches are a promising area of research for power side-channel attacks, and are expected to continue playing an important role in the future.

Table 1 discuss briefly the strengths and limitations of different machine learning approaches for side-channel attacks in both same device and cross-device settings.

6 Future Research Directions for Overcoming Current Challenges

Despite the progress made in machine learning techniques for side-channel attacks, there are still several challenges that need to be addressed. Here are some potential research directions to overcome these challenges:

Robustness Against Adversarial Attacks: While adversarial machine learning techniques have been explored, there is still a need for more robust techniques that can resist sophisticated attacks. One potential direction is to combine multiple defense mechanisms, such as adversarial training, data augmentation, and model compression, to achieve greater robustness.

Generalization to New Devices: Transfer learning and meta learning techniques have shown promise in improving the generalization of side-channel attacks to new devices. However, these techniques still have limitations in scenarios where the devices are significantly different. Future research can explore novel techniques for transferring knowledge across different devices with varying implementations.

Privacy-Preserving Techniques: Federated learning is a promising technique for side-channel attacks while preserving the privacy of individual devices. However, it still requires a large amount of communication between devices, which can be a bottleneck in some scenarios. Future research can explore new techniques for privacy-preserving side-channel attacks that minimize the amount of communication required between devices.

Real-time Side-Channel Attacks: Several machine learning approaches uses in side-channel attacks involve offline training and testing, which may not be practical for real-time scenarios. To address this, future research could explore new approaches for conducting side-channel attacks in real-time, such as online learning and incremental learning. These techniques have the potential to enable real-time side-channel attacks with improved accuracy and efficiency, and could open up new avenues for applications in areas such as embedded systems and internet-of-things devices.

Side-Channel Attacks on Other Cryptographic Algorithms: While much of the existing research on machine learning approaches for side-channel attacks has centered on the AES algorithm, there is a growing need for methods that is applicable to different cryptographic methods as well. To address this, future research could investigate new techniques for conducting side-channel attacks on algorithms such as RSA and Elliptic Curve Cryptography. By expanding the scope of these techniques, researchers can push the boundaries of what is possible in this field and address the challenges associated with attacking a wider range of cryptographic systems.

Overall, these research directions have the potential to advance the recent techniques to enhance the effectiveness of machine learning techniques for SCA.

7 Conclusion

In conclusion, this survey paper has explored the use of machine learning approaches uses power side-channel attacks in cross-device settings. We began by

discussing the basics of side-channel attacks and their relevance in modern-day security, followed by a review of recent research efforts in this field, categorized by the machine learning techniques used and the device settings in which they were tested.

Based on our analysis, we identified several key advantages of these approaches, including the ability to successfully extract secret information from multiple devices with high accuracy, the potential for real-world applications, and the efficiency and versatility of the machine learning techniques. However, there are also several limitations, such as the reliance on quality and quantity of training data, ethical and legal concerns, and the need for further research into generalizability and countermeasures.

Looking ahead, we believe that future research in this area should focus on addressing these limitations and further exploring the latent of machine learning approaches for power SCAs in cross-device settings. This includes developing more robust training data, exploring more ethical and legal ways to conduct experiments, and identifying more effective countermeasures to mitigate the risks of these types of attacks. While deep learning approaches, such as Autoencoder, CNN, and LSTM, show great promise for SCA applications, the presentation of the machine learning approach rely on the specific application and the characteristics of the target device. Therefore, the selection of machine learning approach needs to be carefully considered due to the context of the specific use case. By continuing to explore these avenues, we believe that this field can have a significant impact on improving the security of modern-day devices and systems.

References

1. Cao, P., Zhang, C., Lu, X., Gu, D.: Cross-device profiled side-channel attack with unsupervised domain adaptation. IACR Trans. Cryptograph. Hardw. Embed. Syst. 27–56 (2021)
2. Chapagain, A., Ghimire, A., Joshi, A., Jaiswal, A.: Predicting breast cancer using support vector machine learning algorithm. Int. Res. J. Innov. Eng. Technol. **4**(5), 10 (2020)
3. Das, D., Golder, A., Danial, J., Ghosh, S., Raychowdhury, A., Sen, S.: X-deepSCA: cross-device deep learning side channel attack. In: Proceedings of the 56th Annual Design Automation Conference 2019, pp. 1–6 (2019)
4. Ghimire, A., Tayara, H., Xuan, Z., Chong, K.T.: CSATDTA: prediction of drug-target binding affinity using convolution model with self-attention. Int. J. Mol. Sci. **23**(15), 8453 (2022)
5. Golder, A., Das, D., Danial, J., Ghosh, S., Sen, S., Raychowdhury, A.: Practical approaches toward deep-learning-based cross-device power side-channel attack. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **27**(12), 2720–2733 (2019)
6. Hanley, N., O'Neill, M., Tunstall, M., Marnane, W.P.: Empirical evaluation of multi-device profiling side-channel attacks. In: 2014 IEEE Workshop on Signal Processing Systems (SiPS), pp. 1–6. IEEE (2014)
7. Heuser, A., Zohner, M.: Intelligent machine homicide. In: Schindler, W., Huss, S.A. (eds.) COSADE 2012. LNCS, vol. 7275, pp. 249–264. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29912-4_18

8. Hu, F., Ni, F.: Software implementation of AES-128: side channel attacks based on power traces decomposition. In: 2022 International Conference on Cyber Warfare and Security (ICCWS), pp. 14–21. IEEE (2022)
9. Hu, F., Wang, H., Wang, J.: Cross-subkey deep-learning side-channel analysis. IACR Cryptology ePrint Archive 2021, 1328 (2021)
10. Hu, F., Wang, H., Wang, J.: Side-channel attacks based on power trace decomposition. Cryptology ePrint Archive (2022)
11. Jin, S., Kim, S., Kim, H., Hong, S.: Recent advances in deep learning-based side-channel analysis. ETRI J. **42**(2), 292–304 (2020)
12. Kashyap, P., Aydin, F., Potluri, S., Franzon, P.D., Aysu, A.: 2Deep: enhancing side-channel attacks on lattice-based key-exchange via 2-D deep learning. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **40**(6), 1217–1229 (2020)
13. Koblah, D.S., et al.: A survey and perspective on artificial intelligence for security-aware electronic design automation. ACM Trans. Des. Autom. Electron. Syst. (TODAES) (2022)
14. Meshgi, H., Khazaee, M.E., Kasiri, B., Shahhoseini, H.S.: An efficient algorithm resistant to spa and DPA variants in ECC. In: 2008 1st IFIP Wireless Days, pp. 1–5. IEEE (2008)
15. Patranabis, S., Mukhopadhyay, D.: Fault Tolerant Architectures for Cryptography and Hardware Security. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-1387-4
16. Randolph, M., Diehl, W.: Power side-channel attack analysis: a review of 20 years of study for the layman. Cryptography **4**(2), 15 (2020)
17. Thapar, D., Alam, M., Mukhopadhyay, D.: Deep learning assisted cross-family profiled side-channel attacks using transfer learning. In: 2021 22nd International Symposium on Quality Electronic Design (ISQED), pp. 178–185. IEEE (2021)
18. Wang, H.: Side-channel analysis of AES based on deep learning (2019)
19. Wang, H., Dubrova, E.: Federated learning in side-channel analysis. In: Hong, D. (ed.) ICISC 2020. LNCS, vol. 12593, pp. 257–272. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-68890-5_14
20. Wang, H., Dubrova, E.: Tandem deep learning side-channel attack on FPGA implementation of AES. SN Comput. Sci. **2**, 1–12 (2021)
21. Wolf, S., Hu, H., Cooley, R., Borowczak, M.: Stealing machine learning parameters via side channel power attacks. In: 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 242–247. IEEE (2021)
22. Yu, H., Shan, H., Panoff, M., Jin, Y.: Cross-device profiled side-channel attacks using meta-transfer learning. In: 2021 58th ACM/IEEE Design Automation Conference (DAC), pp. 703–708. IEEE (2021)
23. Yu, H., et al.: Noise2clean: cross-device side-channel traces denoising with unsupervised deep learning. Electronics **12**(4), 1054 (2023)
24. Zhang, L., Xing, X., Fan, J., Wang, Z., Wang, S.: Multilabel deep learning-based side-channel attack. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **40**(6), 1207–1216 (2020)