Domain Adaptation for Side-Channel Analysis Using Deep Reconstruction-Classification Networks

Zhiyuan Xiao[1], Chen Wang[1,4], Tianlong Sun[1], Wenying Zheng[2], Dengzhi Liu[3]*

[1] School of Information Science and Engineering (School of Cyber Science and Technology), Zhejiang Sci-Tech University, China
[2] School of Computer Science and Technology (School of Artificial Intelligence), Zhejiang Sci-Tech University, China
[3] School of Computer Engineering, Jiangsu Ocean University, China
[4] Zhejiang Provincial Innovation Center of Advanced Textile Technology, China
anderson__xiao@163.com, wangchen@zstu.edu.cn, suntl001211@gmail.com, zhengwy0501@126.com, liudz@jou.edu.cn

Abstract

Side-channel analysis (SCA) exploits physical leakages to evaluate cryptographic system security, but traditional methods struggle with cross-device attacks due to hardware variations. This paper introduces a domain adaptation approach using Deep Reconstruction-Classification Networks (DRCN) and Maximum Mean Discrepancy (MMD) loss, enabling knowledge transfer without labeled data. By aligning feature distributions between source and target devices, the DRCN method improves cross-device attack performance. Experiments on datasets, including TinyAES-128 electromagnetic traces and XMEGA data, show significant enhancements. The approach reduces the number of power traces required for key recovery and lowers Guessing Entropy (GE) in cross-device scenarios, increasing attack success rates. In summary, the DRCN-based domain adaptation method offers an effective solution for improving cross-device SCA, demonstrating practical value and efficiency.

Keywords: DLSCA, Joint side-channel analysis, Small sample, AES

1 Introduction

The modeling and analysis of side-channel leakage hold immense potential in the field of research. Firstly, the types of leaked information are diverse. During the computation process of IoT devices, various physical leakages, such as timing delays (timing attacks) [1], power consumption (power attacks) [2], and electromagnetic radiation (electromagnetic attacks) [3], can be exploited. These leakages have given rise to a new study, where researchers combine physical observations of particular internal conditions with assumptions about the manipulated data to recover the intermediate states processed by the device. Secondly, the data volume of leaked information is substantial, requiring a large amount of data for side-channel analysis (SCA). However, relying solely on manual processing often limits speed and accuracy. Especially in the scenarios such as mobile ad hoc network (MANETs) [4] or wireless sensor networks (WSNs) [5], only a limited amount of leaked information can be obtained as small sample datasets due to the high mobility of the target devices. These datasets lead to lower accuracy and efficiency in recovering the keys using the single-input methods.

In light of these considerations, researchers have developed various approaches aimed at improving the accuracy and efficiency of SCA. In recent years, with the rapid development of machine learning, especially deep learning [6], an increasing number of studies have applied machine learning to SCA, yielding better results than traditional analysis methods. For instance, studies like Backes [7] have applied machine learning to SCA on printer sounds. Martinasek et al. [8] proposed an AES SCA method based on neural networks and classified AES keys. Wang et al. [9] proposed a federated learning-based SCA method. Hu et al. [10] introduced a multi-loss regularized denoising autoencoder framework to reduce noise in SCA, thereby reducing the number of traces required for key recovery. These studies clearly emphasize the effectiveness of deep learning techniques in the SCA community.

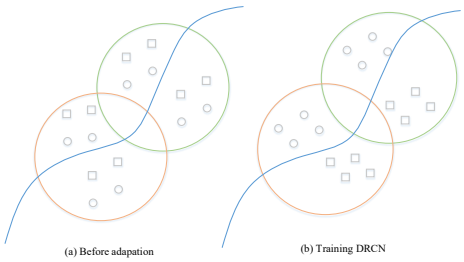


Figure 1. Domain adaptation effects

Recently, Wouters et al. [11] analyzed multiple DST respondents using multilayer perceptrons (MLPs) and found that if only a single device is used for analysis, DLSCAs are challenging to succeed in practice. To enhance to advance the performance of attacks targeting diverse devices in the presence of discrepancies, Das et

*Corresponding Author: Chen Wang; Email: wangchen@zstu.edu.cn
DOI: https://doi.org/10.70003/160792642026092705005

al. [12] combined data processing techniques such as dynamic time warping and principal component analysis, into MLPs. Zhang et al. [13] used deep learning techniques and frequency analysis to address device variability, while Das et al. [12] highlighted the significance of model adaptability in DLSCAs and proposed leveraging training across multiple devices to improve performance. Xiao et al. [14] proposes a joint SCA method, addressing the challenge of recovering keys from limited traces. In summary, these efforts aim to combat non-portability by implementing network architecture changes and utilizing federated target devices. Recently, researchers in the SCA field have been investigating transfer learning (TL) as a potential solution to the portability issue in DLSCA. Several studies have leveraged transfer learning methods to minimize the number of traces needed for effective analysis, as demonstrated in prior research, such as [15-18]. However, these methods still rely on labeled attack traces, which can be difficult to obtain in real-world scenarios. This paper proposes a DRCN-based domain adaptation method that enables transfer learning from source to target devices without the need for labels. The data distribution is very chaotic without domain adaptation, as shown in Figure 1. After applying domain adaptation techniques, the data distribution becomes more aligned and orderly. This illustration demonstrates the effects of domain adaptation, with the left image showing the data distribution before adaptation and the right image displaying the improved alignment after training with DRCN.

The contributions of this paper are as follows:

A DRCN-based unsupervised domain adaptation method is proposed. This paper introduces a domain adaptation technique combining DRCN with the MMD loss function, achieving unsupervised transfer learning from source to target devices in SCA.

The success rate of device-independent attacks is improved. Experimental results demonstrate that this approach greatly enhance the performance of attacks across devices, lowering the required number of power traces for SCA across different devices and boosting the overall attack success rate.

The challenge of obtaining labels in real-world scenarios is solved. Unlike traditional methods that rely on a large number of labeled attack traces, this method effectively performs transfer learning without the need for labels, overcoming the data annotation challenges in practical applications and demonstrating high practical value.

The rest of the paper is structured as follows. Section II provides an introduction to several preliminary concepts, such as an overview of AES, SCA, DRCN. Section III elaborates on the primary method based on DRCN method. Section IV discusses the experimental results and their analysis. Finally, Section V summarizes the main contributions and outlines future research directions.

2 Preliminaries

In this section, we introduce SCA, DRCN, and AES.

2.1 SCA

Side-channel analysis (SCA) was initially introduced by Paul Kocher [1], and he expanded this concept by introducing power analysis [2], a technique that leverages the fact that electronic circuits often exhibit varying power consumption depending on the data they process. Among the various side-channel vulnerabilities, power consumption remains one of the most extensively exploited. This paper focuses predominantly on power analysis and electromagnetic (EM) analysis [19] as primary methods of investigation.

2.2 DRCN

The Deep Reconstruction-Classification Networks (DRCN) [20] integrate the strengths of Convolutional Neural Networks (CNNs) [21] and autoencoders, with a primary focus on domain adaptation tasks. DRCN architecture comprises two main components: a classification branch and a reconstruction branch. The model features an encoder-decoder structure, where the encoder is composed of several convolutional layers and max-pooling layers to extract high-dimensional features. These features are then flattened by a fully connected layer, with a Dropout layer incorporated to mitigate overfitting. The decoder subsequently reconstructs the flattened features into their original data shape using upsampling and additional convolutional layers. The DRCN's loss function is a combination of classification loss and reconstruction loss.

Classification Loss:

$$\mathcal{L}_{\text{cls}} = -\frac{1}{N}\sum_{i=1}^{N} y_i \log(f(x_i)) \tag{1}$$

Reconstruction Loss:

$$\mathcal{L}_{\text{rec}} = \frac{1}{M}\sum_{j=1}^{M} \left\| x_j - g(f(x_j)) \right\|^2 \tag{2}$$

The total loss function is a weighted sum of the classification loss and the reconstruction loss:

$$\mathcal{L} = \mathcal{L}_{\text{cls}} + \lambda \mathcal{L}_{\text{rec}} \tag{3}$$

By minimizing this combined loss, the DRCN aligns data from the source and target domains more closely within the feature space, thereby improving cross-dataset attack performance. This alignment is crucial for domain adaptation, as it ensures that the model trained on source domain data can generalize effectively to the target domain. Additionally, the model's robustness and accuracy in various domain adaptation scenarios can be further enhanced by incorporating other regularization techniques or alternative loss functions, such as adversarial loss. Figure 2 illustrates the structure of DRCN.

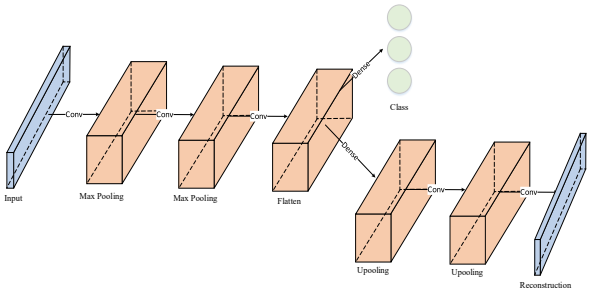


Figure 2. DRCN structure

2.3 AES

The Advanced Encryption Standard (AES) [22] is one of the most widely used symmetric encryption algorithms, designed to secure electronic data through encryption. Since the public dataset used in this study is encrypted with AES-128, we focus on this encryption specification for our analysis.

3 DRCN Method

In this section, the DRCN method are introduced in detail.

3.1 Device Differentiation

In SCA, differences between devices primarily arise from the following aspects, making it challenging to effectively attack data collected from one device on another. First, subtle differences in hardware implementation and manufacturing processes exist between devices. Even for devices of the same model, each device's hardware characteristics (such as resistance, capacitance, and transistor properties) are not identical due to unavoidable manufacturing tolerances and material variations during production. These minor hardware differences can result in varying electromagnetic emissions and power consumption patterns during the execution of identical encryption operations.

Additionally, differences in operating environments can affect the characteristics of side-channel signals. For instance, environmental factors such as temperature, humidity, fluctuations in power supply voltage, and surrounding electromagnetic interference can influence the device's power consumption traces. Variations in these external conditions further exacerbate the differences between devices of the same model. Mathematically, this difference can be represented by the data distributions $P_s(x)$ for the source device and $P_t(x)$ for the target device. Typically, these distributions are not identical, i.e., $P_s(x) \neq P_t(x)$. The difference in distributions creates difficulties in transferring a model ($f(x|\theta)$ trained on the source device to the target device, as the features learned from the source device fail to adapt effectively to the target device.

Moreover, the signal acquisition process also introduces variations. Differences in measurement equipment, probe placement, and signal amplifiers can all affect the collected side-channel signals. These variations in the measurement process can result in differences in the collected signals even for the same device across different experiments. Differences in hardware implementation, changes in operating environments, and inconsistencies in the measurement process are the primary causes of variations in side-channel signals between different devices. These differences make it difficult to perform effective SCA on a different device using a model trained on one device, compelling researchers to seek domain adaptation techniques to address this issue.

3.2 DRCN Method

In SCA, substantial differences between devices or datasets can pose challenges for a model trained on one dataset to generalize effectively to another. To mitigate this issue, domain adaptation techniques are employed to reduce the distributional gap between the source domain (training data) and the target domain (testing data). The Deep Reconstruction-Classification Network (DRCN) is a deep learning model that combines the strengths of Convolutional Neural Networks (CNN) and Residual Networks (ResNet), making it well-suited for complex feature extraction and pattern recognition tasks.

In DRCN, the Maximum Mean Discrepancy (MMD) [23] loss function is utilized to facilitate domain adaptation. MMD is a statistical measure designed to quantify the distance between two probability distributions. Theoretically, if two distributions are identical, their MMD value is zero; any differences between them result in a positive MMD value. The core principle of MMD involves identifying a specific function within a function space that maximizes the expected difference in outputs between the two distributions. This function space is typically a Reproducing Kernel Hilbert Space (RKHS), where each function is associated with a kernel function. The use of kernel functions significantly simplifies the computation of differences between distributions.

The calculation formula for MMD is given by:

$$\mathcal{D}_{\mathrm{MMD}}[\mathcal{R}, p, q] = \sup_{\substack{f \in \mathcal{R} \\ \|f\|_{\mathcal{H}} \leq 1}} \left| \mathbb{E}_{u \sim p}[f(u)] - \mathbb{E}_{v \sim q}[f(v)] \right| \tag{4}$$

where sup represents the supremum, or the least upper bound, of the set, used to identify the function f within the function space $\mathcal{R}$ that maximizes the subsequent expression. The term $\left|\mathbb{E}_p[f(x)] - \mathbb{E}_q[f(y)]\right|$ signifies the absolute difference between the expected values under the two distributions, highlighting the discrepancy between the probability distributions p and q.

In practice, MMD is computed using sample sets $D_u = \{u_i\}_{i=1}^n$ and $(D_v = \{v_i\}_{i=1}^n$ drawn from two probability distributions p and q respectively, where n and m denote the number of samples in each set. The squared form of MMD can be expressed as follows:

$$\mathcal{D}^2_{\text{MMD}} = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{i'=1}^{n}k(u_i,u_{i'}) - \frac{2}{nm}\sum_{i=1}^{n}\sum_{j=1}^{m}k(u_i,v_j) + \frac{1}{m^2}\sum_{j=1}^{m}\sum_{j'=1}^{m}k(v_j,v_{j'}) \quad (5)$$

where $k(u_i,u_{i'}) = \langle\psi(u_i),\psi(u_{i'})\rangle_{\mathcal{H}}$ represents the inner product between two sample points u_i and u_j transformed by the mapping function ψ in the RKHS, encapsulating the geometric similarity of samples in the feature space.

In DRCN, features for the source and target domains are initially extracted through the network, with f_s and f_t representing the feature representations for the source and target domains, respectively. The extracted feature representations are then used to compute the MMD loss between the source and target domains. The MMD loss function can be formulated as:

$$\text{MMD}^2(X_s,X_t) = \left\| \frac{1}{n_s}\sum_{i=1}^{n_s}\phi(x_s^i) - \frac{1}{n_t}\sum_{j=1}^{n_t}\phi(x_t^j) \right\|^2_{\mathcal{H}} \quad (6)$$

where ϕ is the kernel function mapped to the feature space (e.g., Gaussian kernel), and $\mathcal{H}$ denotes the Hilbert space of the feature space.

Finally, the MMD loss is combined with the original classification loss to form the total loss function for optimizing model parameters. The total loss function can be expressed as:

$$\mathcal{L} = \mathcal{L}_{\text{cls}} + \lambda \cdot \text{MMD}^2(f_s,f_t) \quad (7)$$

where $\mathcal{L}_{\text{cls}}$ denotes the classification loss (e.g., cross-entropy loss), and λ is the hyperparameter that balances the MMD loss and classification loss. During training, both classification loss and MMD loss are minimized through backpropagation, allowing the model to perform effective classification on the source domain while also reducing the distributional discrepancy between the source and target domains, thereby achieving domain adaptation. In this way, DRCN combined with MMD loss can be effectively used for cross-dataset SCA, improving attack performance across different devices.

This framework demonstrates how domain adaptation through MMD can bridge the gap between disparate datasets, ensuring the model's robustness and generalization capability in varied environments.

The procedure outlined in Table 1 can be summarized as follows: Initially, the autoencoder (AE) [24] and classifier (C) are initialized. The AE and C are then pre-trained on the source domain data D_S, focusing on minimizing both reconstruction and classification losses. During the domain adaptation phase, in each epoch, the encoder from AE is utilized to extract features from both the source domain and target domain data D_T, resulting in feature representations F_S and F_T. The goal is to minimize the combined loss, which includes the reconstruction loss of the AE, the classification loss of C on the source domain, and the Maximum Mean Discrepancy (MMD) loss between the source and target domains. Finally, the parameters of AE and C are updated, and the classifier's performance is evaluated on the target domain data.

Table 1. The algorithm of unsupervised domain adaptation with DRCN-MMD

Algorithm 1	Unsupervised domain adaptation with DRCN-MMD
Input	Source domain labeled data $D_S = \{(X_{i,S}, Y_{i,S})\}$, Target domain unlabeled data $DT = \{X_{i,T}\}$
Output	Trained classifier C on the target domain
Step 1	Initialize autoencoder AE and Classifier C
Step 2	Pre-train AE and C on D_s by minimizing reconstruction and classification loss
Step 3	For each epoch in domain adaptation: 1. Extract features F_S from D_S and F_T from D_T using AE's encoder. 2. Minimize combined loss: reconstruction loss for AE, classification loss for C on D_S, and MMD loss between F_S and F_T.
Step 4	Update AE and C parameters.
Step 5	Test C using D_T.

4 Experimental Results and Analysis

In this section, we first outline our experimental conditions. We evaluate the proposed joint SCA model using traces obtained from the CW308T-STM32F3 board [25], as shown in Figure 3, and further validate its effectiveness on the dataset captured by the STM32F303. The main hardware configuration also includes an Intel(R) Core(TM) i7-9750H CPU @2.60GHz and an NVIDIA GeForce GTX 4090 6GB GPU, used for numerical calculations and model training tasks.

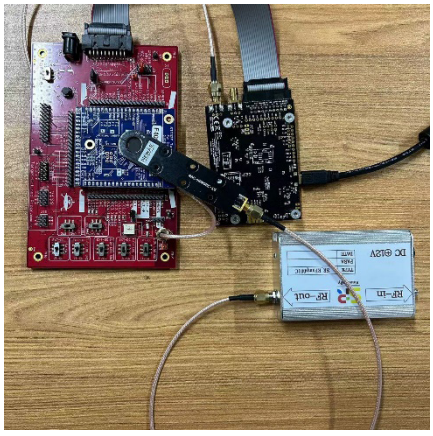


Figure 3. Capture device

4.1 Experimental Results

In this work, we utilized the DRCN combined with the MMD loss function [26] for domain adaptation in SCA. This approach seeks to optimize the efficiency of attacks across devices and assess its performance across diverse device configurations.

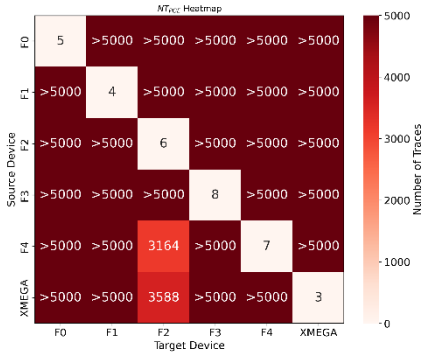


Figure 4. High trace requirements for cross-device attacks without domain adaptation

Figure 4 illustrates the Guessing Entropy (GE) [27] of traditional SCA methods on different devices. Each square in the figure represents the GE value for a source and target device combination, with darker colors indicating higher GE values and greater attack difficulty. It can be observed that when the same device serves as both the source and target, fewer power traces are needed for successful key recovery (as indicated by the lighter regions along the diagonal), requiring approximately 10 traces. However, for attacks between different devices (off-diagonal regions), the GE value increases significantly, demonstrating the lower effectiveness of traditional methods in cross-device attacks, with key recovery being unsuccessful in most cases.

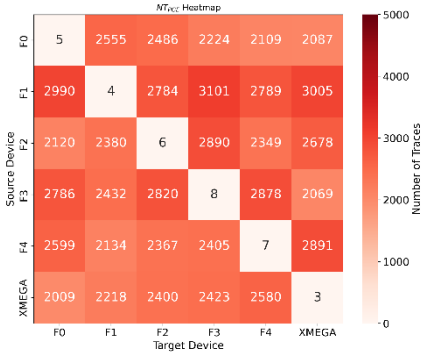


Figure 5. Reduced trace requirements after applying DRCN domain adaptation, improving cross-device attack efficiency

To boost the efficacy of attacks across various devices, we employed a domain adaptation method based on the MMD loss function. After preprocessing, the data characteristics of the target domain become more aligned with those of the source domain. Figure 5 shows the GE of cross-device attacks after calibration, with a noticeable reduction in GE values and lighter colors. This indicates that domain adaptation significantly enhances cross-device attack performance, achieving near single-device attack effectiveness in some cases. Notably, for attacks between different devices, the GE value decreases substantially, reflecting a higher attack success rate.

To further validate our domain adaptation method, we performed comprehensive experiments on the XMEGA dataset. For training, 20,000 traces were employed, 5,000 traces were set aside for validation, 100 traces were designated for fine-tuning, and another 5,000 traces were reserved for attack evaluation. As shown in Figure 5, the results of the model prior to adaptation varied across different devices. However, the fine-tuned model successfully recovered keys from all devices using only 100 attack traces. Figure 5 also presents the changes in test loss and validation MMD loss, emphasizing that reducing the MMD loss significantly lowers the test loss on the target device.

Through these experiments, the performance of the DRCN network combined with the MMD loss function for cross-device SCA has been validated. This approach significantly enhances cross-device attack performance and provides an effective domain adaptation solution. The comparison results in Figure 4 and Figure 5 clearly demonstrate the significant differences in attack performance before and after calibration, further proving the efficacy of domain adaptation techniques in addressing distributional discrepancies between side-channel data from different devices. This study shows that employing the Deep Residual Convolutional Network and MMD loss function for domain adaptation can substantially improve cross-device SCA effectiveness, reduce the number of required power traces, and enhance attack success rates, offering a new and effective method for SCA.

5 Conclusion

This paper presents a novel domain adaptation approach in SCA, utilizing DRCN in conjunction with the MMD loss function. The proposed method effectively addresses the challenges associated with cross-device attacks by aligning data distributions between source and target domains, thereby significantly enhancing attack performance and reducing the number of required power traces. Experimental results demonstrate that the DRCN-MMD framework surpasses traditional methods, achieving near single-device attack effectiveness even across varying devices. Looking ahead, future work could explore integrating multiple domains into a unified training framework to further improve cross-device performance. Combining data from diverse sources and employing multi-domain training approaches could yield even more robust domain adaptation solutions. Additionally, incorporating techniques such as federated learning could facilitate model training on multiple datasets while preserving data privacy. Expanding the method to address more complex scenarios, such as varying environmental conditions and hardware configurations, will be crucial for advancing the practical applicability of domain adaptation in SCA. These future directions hold the promise of enhancing

the generalization and effectiveness of SCA, paving the way for more sophisticated and resilient security analysis techniques.

6 Acknowledgement

The work is supported by the National Key R&D Program of China (No. 2023YFB2703700), the National Natural Science Foundation of China (Nos. U21A20465, 62302457, 62402444, 62102169), the Fundamental Research Funds of Zhejiang Sci-Tech University (No. 22222266-Y), the Program for Leading Innovative Research Team of Zhejiang Province (No. 2023R01001), the Zhejiang Provincial Natural Science Foundation of China (Nos. LQ24F020008, LQ24F020012), and the "Pioneer" and "Leading Goose" R&D Program of Zhejiang (No. 2023C01119).

References

[1] P. C. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, *Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference*, Santa Barbara, California, USA, 1996, pp. 104–113. https://doi.org/10.1007/3-540-68697-5_9

[2] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, *Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference*, Santa Barbara, California, USA, 1999, pp. 388–397. https://doi.org/10.1007/3-540-48405-1_25

[3] K. Gandolfi, C. Mourtel, F. Olivier, Electromagnetic analysis: Concrete results, *Cryptographic Hardware and Embedded Systems—CHES 2001: Third International Workshop*, Paris, France, 2001, pp. 251–261. https://doi.org/10.1007/3-540-44709-1_21

[4] J. Shen, Z. Gui, X. Chen, J. Zhang, Y. Xiang, Lightweight and certificateless multi-receiver secure data transmission protocol for wireless body area networks, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 3, pp. 1464–1475, May-June, 2022. https://doi.org/10.1109/TDSC.2020.3025288

[5] C. Wang, T. Zhou, J. Shen, W. Wang, X. Zhou, Searchable and secure edge pre-cache scheme for intelligent 6G wireless systems, *Future Generation Computer Systems*, Vol. 140, pp. 129–137, March, 2023. https://doi.org/10.1016/j.future.2022.10.012

[6] I. Goodfellow, Y. Bengio, A. Courville, *Deep Learning*, MIT Press, Cambridge, 2016.

[7] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, C. Sporleder, Acoustic side-channel attacks on printers, *19th USENIX Security Symposium (USENIX Security 10)*, Washington, DC, USA, 2010.

[8] Z. Martinasek, V. Zeman, Innovative method of the power analysis, *Radioengineering*, Vol. 22, No. 2, pp. 586–594, June, 2013.

[9] H. Wang, E. Dubrova, Federated learning in side-channel analysis, *Information Security and Cryptology–ICISC 2020: 23rd International Conference*, Seoul, South Korea, 2020, pp. 257–272. https://doi.org/10.1007/978-3-030-68890-5_14

[10] F. Hu, J. Shen, P. Vijayakumar, Side-channel attacks based on multi-loss regularized denoising autoencoder, *IEEE Transactions on Information Forensics and Security*, Vol. 19, pp. 2051–2065, 2024. https://doi.org/10.1109/TIFS.2023.3343947

[11] L. Wouters, J. Van den Herrewegen, F. D. Garcia, D. Oswald, B. Gierlichs, B. Preneel, Dismantling DST80-based immobiliser systems, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, Vol. 2020, No. 2, pp. 99–127, March, 2020. https://doi.org/10.13154/tches.v2020.i2.99-127

[12] D. Das, A. Golder, J. Danial, S. Ghosh, A. Raychowdhury, S. Sen, X-deepsca: Cross-device deep learning side channel attack, *Proceedings of the 56th Annual Design Automation Conference*, Las Vegas, NV, USA, 2019, pp. 1–6.

[13] F. Zhang, B. Shao, G. Xu, B. Yang, Z. Yang, Z. Qin, K. Ren, From homogeneous to heterogeneous: Leveraging deep learning-based power analysis across devices, *2020 57th ACM/IEEE Design Automation Conference (DAC)*, San Francisco, USA, 2020, pp. 1–6.

[14] Z. Xiao, C. Wang, J. Shen, Q. M. J. Wu, D. He, Less Traces Are All It Takes: Efficient Side-Channel Analysis on AES, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 44, No. 6, pp. 2080-2092, June, 2025. https://doi.org/10.1109/TCAD.2024.3518414

[15] C. Genevey-Metat, A. Heuser, B. Gérard, Train or adapt a deeply learned profile? *Progress in Cryptology–LATINCRYPT 2021: 7th International Conference on Cryptology and Information Security*, Bogotá, Colombia, 2021, pp. 213–232. https://doi.org/10.1007/978-3-030-88238-9_11

[16] D. Thapar, M. Alam, D. Mukhopadhyay, Transca: Cross-family profiled side-channel attacks using transfer learning on deep neural networks, *Cryptology ePrint Archive*, Article No. 2020/1258, October, 2020. https://eprint.iacr.org/2020/1258

[17] H. Yu, H. Shan, M. Panoff, Y. Jin, Cross-device profiled side-channel attacks using meta-transfer learning, *2021 58th ACM/IEEE Design Automation Conference (DAC)*, San Francisco, CA, USA, 2021, pp. 703–708. https://doi.org/10.1109/DAC18074.2021.9586100

[18] H. Wang, M. Brisfors, S. Forsmark, E. Dubrova, How diversity affects deep-learning side-channel attacks, *2019 IEEE Nordic Circuits and Systems Conference (NORCAS): NORCHIP and International Symposium of System-on-Chip (SoC)*, Helsinki, Finland, 2019, pp. 1–7. https://doi.org/10.1109/NORCHIP.2019.8906945

[19] F.-X. Standaert, Introduction to side-channel attacks, in: I. Verbauwhede (Eds.), *Secure Integrated Circuits and Systems*, Springer, Boston, 2010, pp. 27–42. https://doi.org/10.1007/978-0-387-71829-3_2

[20] M. Ghifary, W. B. Kleijn, M. Zhang, D. Balduzzi, W, Li, Deep reconstruction-classification networks for unsupervised domain adaptation, *Computer Vision–ECCV 2016: 14th European Conference*, Amsterdam, The Netherlands, 2016, pp. 597–613. https://doi.org/10.1007/978-3-319-46493-0_36

[21] R. Benadjila, E. Prouff, R. Strullu, E. Cagli, C. Dumas, Deep learning for side-channel analysis and introduction to ASCAD database, *Journal of Cryptographic Engineering*, Vol. 10, No. 2, pp. 163–188, June, 2020. https://doi.org/10.1007/s13389-019-00220-8

[22] J. Daemen, V. Rijmen, *The Design of Rijndael*, Springer, 2002.

[23] H. Yan, Y. Ding, P. Li, Q. Wang, Y. Xu, W. Zuo, Mind the

class weight bias: Weighted maximum mean discrepancy for unsupervised domain adaptation, *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Honolulu, HI, USA, 2017, pp. 945–954. https://doi.ieeecomputersociety.org/10.1109/CVPR.2017.107

[24] J. Liu, G. Xie, J. Wang, S. Li, C. Wang, F. Zheng, Y. Jin, Deep industrial image anomaly detection: A survey, *Machine Intelligence Research*, Vol. 21, No. 1, pp. 104–135, February, 2024. https://doi.org/10.1007/s11633-023-1459-z

[25] C. O'Flynn, Z. Chen, Chipwhisperer: An open-source platform for hardware embedded security research, *Constructive Side-Channel Analysis and Secure Design: 5th International Workshop (COSADE 2014)*, Paris, France, 2014, pp. 243–260. https://doi.org/10.1007/978-3-319-10175-0_17

[26] P. Cao, C. Zhang, X. Lu, D. Gu, Cross-device profiled side-channel attack with unsupervised domain adaptation, *IACR Transactions on Cryptographic Hardware and Embedded Systems*, Vol. 2021, No. 4 pp. 27–56, August, 2021. https://doi.org/10.46586/tches.v2021.i4.27-56

[27] F.-X. Standaert, T. G. Malkin, M. Yung, A unified framework for the analysis of side-channel key recovery attacks, *Advances in Cryptology—EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cologne, Germany, 2009, pp. 443–461. https://doi.org/10.1007/978-3-642-01001-9_26

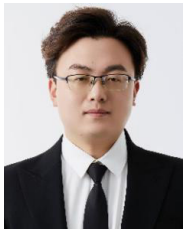
Biographies

Zhiyuan Xiao received his B.S. degree from Gannan University of science and technology, Ganzhou, China, in 2021. He is currently pursuing a master's degree at Zhejiang Sci-Tech University, Hangzhou, China. His research interests include hardware encryption and side channel analysis.

Chen Wang received the Ph.D. degree at Nanjing University of Information Science and Technology, Nanjing, China, in 2022. He is an Associate Professor in the Zhejiang Sci-Tech University, Hangzhou, China. His research interests include secure data aggregation, edge computing security, and AI-enabled security.

Tianlong Sun received his B.S. degree from Zhejiang Sci-tech University, Hangzhou, China, in 2022. He is currently pursuing a master's degree at Zhejiang Sci-Tech University, Hangzhou, China. His research interests include deep learning and side channel analysis.

Wenying Zheng received the Ph.D. degree in computer science from Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2022. She is currently working with the School of Computer Science and Technology, Zhejiang Sci-Tech University, Hangzhou, China. Her research interests include cloud storage security, security systems, and network security.



Dengzhi Liu received the M.E. degree and Ph.D. degree from Nanjing University of Information Science and Technology in 2020. He is currently an Associate Professor with Jiangsu Ocean University, China. His current research interests include data security and cyber security.