PRIDES: A Power Rising Descending Signature for Improving IoT Security

Ashish Mahanta and Haibo Wang
School of Electrical, Computer, and Biomedical Engineering
Southern Illinois University, Carbondale, IL 62901, USA

***Abstract*—This work presents a novel digital signature to characterize the rising and descending patterns of IoT device power consumption, which can be used to detect abnormal operations. The digital signature, referred to as PRIDES, can be generated using simple digital-like circuits and hence incurs very low hardware overhead. A novel PRIDES generation circuit is implemented with a 90 nm CMOS technology and its operation is validated via transistor-level simulation. A PRIDES-based methodology to detect the insertion of potentially malicious codes is presented and its effectiveness is demonstrated with using power consumption data measured from hardware experiments.**

***Index Terms*—Internet of Things (IoT), hardware security, power signature**

I. INTRODUCTION

The Internet of Things (IoT) refers to the fast-growing networked devices that incorporate capabilities of communication, computing, sensing, and actuation. These devices have widely infiltrated into almost all the fields of society, such as manufacturing, agriculture, medicare, smart grids, autonomous vehicles, smart homes, etc. [1]–[6]. The burgeoning IoT market size is expected to grow from USD 384.70 billion in 2021 to USD 2.47 trillion by 2029 [7]. As the number and application of IoT devices proliferate rapidly, it raises many security and privacy concerns, particularly for the devices handling sensitive data or carrying out mission-critical functions. Recently, a number of high-profile cyber attacks on IoT devices had grabbed the world's attention and exemplified the importance to safeguard the integrity of IoT devices. Such examples include the Verkada breach, the Florida water facility attack, and the Colonial Pipeline attack, all in 2021. It was reported that IoT is regarded as the next big hacking prize by the dark web's criminal minds [8].

Most IoT devices have limited computation power due to their stringent constraints on energy consumption, device size, and cost. This hampers the capability for implementing advanced encryption, authentication, or other computationally intensive countermeasures on IoT devices. The fact that many IoT devices operate in remote, unprotected environments further exacerbates the challenge of IoT security. In literature, various IoT security techniques have been proposed from different aspects, from hardware design, application development, and network monitoring, up to the perception layer, to address this daunting challenge. Several articles [9]–[11] provide excellent reviews of these techniques. Among them, power analysis has been demonstrated as an effective tool for both malicious players to steal IoT secrets (e.g. encryption keys) and security engineers to detect abnormal operations. The latest development in this front are further discussed in the next section.

Existing power analysis methods depend upon accurately capturing the device power trace, which typically involves bench instrumentation, e.g. oscilloscope, data acquisition (DAQ) boards or analog to digital converters (ADC), as shown in Figure 1. Such methods can achieve high accuracy, but require bulky and power-hungry measurement equipment, making them unsuitable to be integrated into IoT devices. Although some IoT designs may have built-in power monitoring circuits, the requirement of digitizing the captured power consumption signals often leads to large hardware overhead. More importantly, the digital data obtained from these methods typically have a large volume, which is suitable for statistical analysis but not concise enough for being used as signatures.

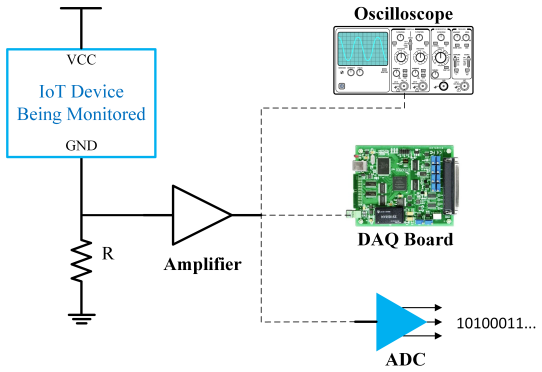


Fig. 1: Typical setup for power trace capturing

This work presents a *p*ower *ri*sing *de*cending *s*ignature, referred to as PRIDES, to depict the power fluctuation patterns during device operation. Using data from hardware experiments, we demonstrate that PRIDES can be used to detect inserted malicious codes into microcontroller units (MCU). A novel PRIDES generation circuit is also developed using a 90 nm CMOS technology and its operation is validated via transistor-level circuit simulation. The proposed circuit has a simple digital-like structure, hence resulting in very small hardware overhead.

The rest of the paper is organized as follows: Section 2 discusses related work on power analysis for IoT security. The proposed methodology and how it is used for malicious code

detection are presented in Section 3. The proposed PRIDES generation circuit is also presented in this section. Section 4 presents the experimental results and the paper is concluded in Section 5.

II. RELATED WORK

Power analysis has been demonstrated as a potent tool in the toolbox of side-channel attacks (SCA) [12], [13]. It leverages statistical or machine learning methods to exploit subtle changes in power dissipation associated with various control paths, different arithmetic operations, or variations of data involved in the computation. Differential power analysis has been successfully used to reveal encryption keys and other device secrets [14]–[16]. Recently, power analysis was studied for disassembling instructions being executed in MCU. The works presented in [17]–[20] have achieved impressive success rates in identifying individual instructions with the help of advanced data analysis techniques, such as linear discriminant analysis, quadratic discriminant analysis, hidden Markov models, principal component analysis, k-nearest neighbors algorithm, etc.

By the same token, power analysis can also be used to detect malicious codes, hardware Trojans, and other abnormalities. In [21], [22], statistical features extracted from power trace data, including mean, variance, skewness, kurtosis, L2-norm error, permutation entropy, and data smashing distance, are used to detect malware on computers. Hardware Trojans can also be exposed via power analysis based statistical learning approaches [23] or transient current analysis [24].

Generally speaking, the success of the aforementioned methods depends on the capability of capturing large volumes of power trace data with high accuracy. This demands complicated power trace capturing setups, often involving bench instrumentation or high-precision data acquisition circuits. Also, the advanced data analysis involved in these methods is computationally intensive. Hence, the existing methods are more suitable for being used at the server ends or performing offline analysis. It is challenging to deploy these methods on IoT devices and detect abnormalities on the fly.

III. PROPOSED METHODOLOGY

Motivated by the above observations, this work presents a concise signature to characterize the rising and descending patterns of device power dissipation. In PRIDES, a single bit, b_i, is used to indicate if the power consumption is rising ($b_i = 1$) or descending ($b_i = 0$) at sampling time t_i. PRIDES can be generated by a simple digital-like circuit without involving sophisticated data acquisition circuits or ADCs. Hence, it incurs much smaller hardware overhead compared to existing power trace capturing circuits. It is envisioned that PRIDES can be used to assess the fidelity of critical operations or computation tasks on IoT devices, in a way similar to using digital signatures to verify the authenticity of electronic documents.

The proposed methodology is illustrated in Figure 2. A shunt resistor is used to sense the current dissipated by the MCU or embedded cores of the IoT device. The voltage across the resistor is amplified before feeding to the proposed PRIDES generation circuit. Note that the use of a shunt sensing resistor and amplifier is almost universal in all power trace capturing circuits. One of the unique contributions of this work is the much simplified digital-like PRIDES generation circuit, which will be described in Section 3.A. To capture PRIDES for a selected IoT operation, the MCU or embedded core first enables the PRIDES circuit and then carries out the selected operation. After the completion of the operation, the MCU or embedded core reads back the PRIDES. Since the captured signature is compact (one bit per sample v.s. multi-bits per sample in conventional power traces), the PRIDES bit streams can be appended as a special section of the data packages, which will be transmitted to remote servers for further analysis. Also, the PRIDES can be analyzed by the IoT device to assess the fidelity of the operation in the field. This is further elaborated in Section 3.B.

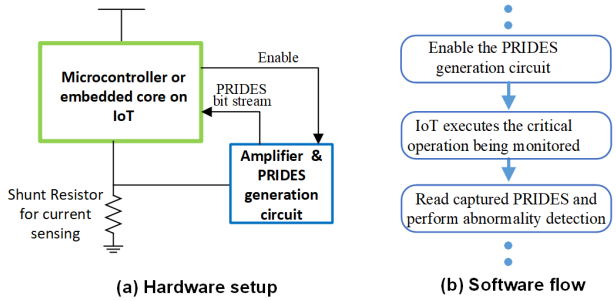


Fig. 2: Using PRIDES to monitor IoT operation fidelity

A. Proposed PRIDES generation circuit

The proposed PRIDES generation circuit is depicted in Figure 3. Its first stage, consisting of M1-M4 and C1, senses the rising or descending trend between two consecutive samples, which are the voltage levels before and after the falling edge of clock signal clk. When $clk = 1$, M2 is conducting which shorts the input and output of the inverter comprised of M3 and M4. This forces the inverter to the operation point that manifests the largest slope on the input-output voltage transfer curve of the inverter. The voltage level of this operating point is often called as the inverter gate threshold voltage V_M. After M2 is off, any small voltage deviations from V_M on the inverter input will cause large voltage variations at the inverter output, making the inverter to behavior like a gain stage. Before the falling edge of clk, capacitor C1 is charged to $V_{psc}^1 - V_M$, where V_{psc}^1 is the output of the amplifier and superscript 1 indicates $clk = 1$.

After clk switches to 0, the inverter input is disconnected from its output and the right terminal of C1 becomes floating. Hence, voltage changes $\Delta V = V_{psc}^0 - V_{psc}^1$ (superscript 0 indicates $clk = 0$) at the left terminal of C1 is passed to the inverter input and subsequently causes a large voltage change at the inverter output. Note that the polarity of ΔV indicates the rising and descending trend of V_{PSC}. For a rising trend

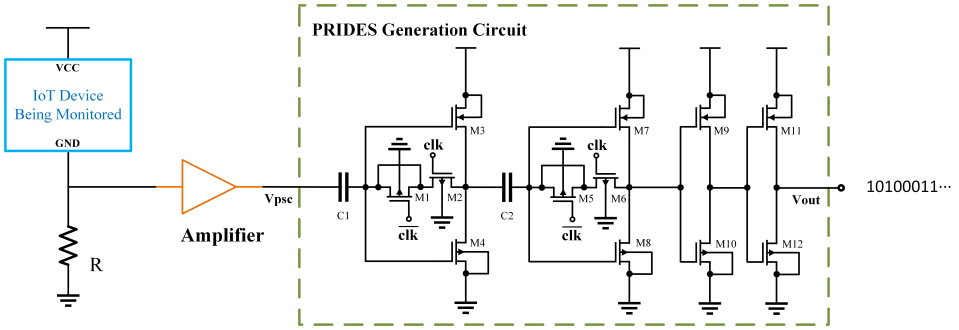


Fig. 3: PRIDES generation circuit

($\Delta V > 0$), the inverter output will swing toward low voltage; otherwise, the inverter output will swing toward high voltage. To mitigate the effect of channel charge injection caused by turning off M2, a dummy device M1 is added and $\overline{clk}$ is a slightly delayed version of the complement of clk.

For small ΔV values, the output swing of the first stage may not be large enough to reach well defined logic levels. Hence, a second stage consisting of M5-M8 and C2 is added to further amplify the output of the first stage. The two following inverters (M9-M10 and M11-M12) are purely digital gates which reshape the output of the second stage to perfect logic level by exploiting the regenerative properties of CMOS logic gates. Hence, the outputs of the PRIDES generation circuit is sequence of binary bits that characterize the rising and descending patterns of the device power consumption.

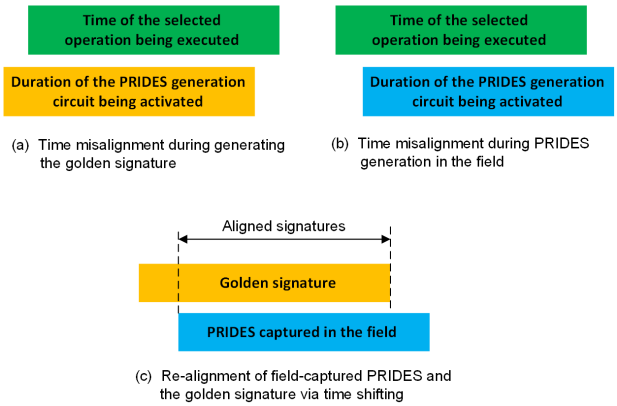


Fig. 4: PRIDES alignment via time shifting

B. PRIDES analysis method

Unlike conventional power traces which are series of values (current dissipation readings) represented in the binary format, PRIDES is a serial bit stream sequence with each bit representing an event (current dissipation rising or descending) at a given sampling time. Thus, PRIDES can be analyzed using much more computation-efficient methods compared to the analysis of conventional power traces. For a given operation to be monitored, the PRIDES of the intact operation is obtained before the IoT deployment. This will be the golden signature $\mathcal{S}$ to be used in later analysis. After a PRIDES, denoted as $\mathcal{P}$, is captured for the same function during field operation, the difference between $\mathcal{S}$ and $\mathcal{P}$ can be examined to assess the fidelity of the selected operation.

Considering time uncertainties associated with IoT operations, the instance that the IoT starts to execute the selected operation and the time that the PRIDES generation circuit starts to capture signatures may not be perfectly synchronized. As a result, $\mathcal{S}$ and $\mathcal{P}$ may not be completely aligned with respect to the instructions of the selected operation as illustrated in Figure 4. To mitigate this problem, we propose to use a normalized time-shifted cross correlation, denoted as ζ, to measure the difference between $\mathcal{S}$ and $\mathcal{P}$.

Algorithm 1 Computing ζ_{max} for $\mathcal{S}$ and $\mathcal{P}$

1: $\zeta_{max} = 0$
2: **for** $k = -n : 1 : n$ **do**
3: **if** $k <= 0$ **then**
4: $A = \mathcal{S}[0 : m + k - 1]$
5: $B = \mathcal{P}[-k : m]$
6: **else**
7: $A = \mathcal{S}[k : m]$
8: $B = \mathcal{P}[0 : m - k - 1]$
9: $t = x\_corr(A, B)/len(A)$
10: $\zeta_{max} = max(\zeta_{max}, t)$

Assume the length of both $\mathcal{S}$ and $\mathcal{P}$ is m bits and the maximum bits to be shifted in the search of the maximum of ζ is n bit. The procedure to compute ζ_{max} is described by Algorithm 1. Lines 4-5 correspond to the scenarios that the capturing time of golden signal $\mathcal{S}$ is ahead of the time of PRIDES $\mathcal{P}$ as illustrated in Figure 4 (c). Lines 7-8 cover the opposite scenarios. A and B obtained from these lines are the presumably aligned signatures in the examination. Function $x\_corr(A, B)$ in line 9 computes the cross correlation between A and B. In the computation, if $A[i] = B[i]$, the result for bit i is 1; otherwise, it is -1. The final cross correlation value is the summation of the results from all the bits. Also, $len(A)$

represents the length of A. Due to the time shifting operation depicted by lines 3-8, the length of A and B varies. Hence, the cross correlation is normalized by the vector length to abate the effect of vector length fluctuation.

IV. EXPERIMENTAL RESULTS

To evaluate the proposed methodology, hardware experiments were conducted to collect power consumption data related to the intact and compromised MCU software routines. The obtained data were then used as the input of the proposed PRIDES generation circuit in SPICE simulation. The cross correlations between the golden signature and the PRIDES obtained from simulation were calculated. It demonstrates the proposed method can distinctly detect compromised MCU software routines.

A. Experiment setup

Figure 5 shows the hardware setup for capturing power consumption data. The MCU used in the experiment are Microchip PIC24F devices. A small shunt resistor is inserted into the MCU ground path for sensing its current consumption. A two-stage amplifier circuit whose schematic is shown in the bottom portion of the figure is used to amplify the voltage across the shunt resistor. The gain and the -3dB bandwidth of the amplifier are 52.5 dB and 330 kHz, respectively. The amplifier output is captured a Diligent Analog Discovery 2 device. The saved data will be used as the input of the PRIDES generation circuit in later circuit simulation. The use of the Diligent Analog Discovery 2 device is because the proposed PRIDES generation circuit has not been implemented in silicon. Once the proposed circuit is fabricated, the PRIDES generation circuit can be directly connected to the amplifier output as shown in Figure 3.

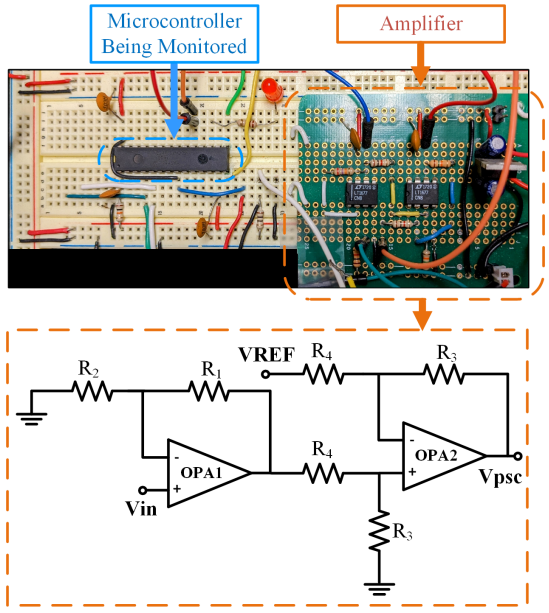


Fig. 5: Hardware setup for capturing power consumption data

The MCU codes shown in Figure 6 are used to emulate the intact and compromised operation. The pristine code displayed in the left portion of the figure performs a vector addition. Before starting the addition operation, an output pin, named as psc_enable, is pulled to high for enabling power dissipation data collection. In the compromised code shown in the right portion of the figure, additional operations are executed when vector bit index k is within the range of (g, h). In the experiments, the values of j, g, and h are 750, 200, and 250, respectively.

Two PIC24F microcontrollers, referred to as $MCU1$ and $MCU2$, were experimented in the study. 100 power traces were captured for each MCU. 50 of them correspond to the scenarios of the pristine code being executed; the other 50 are for the situations that the compromised code was running. The obtained 200 traces of power dissipation data are then used as the input of the PRIDES generation circuit in circuit simulation, which is described as follows.

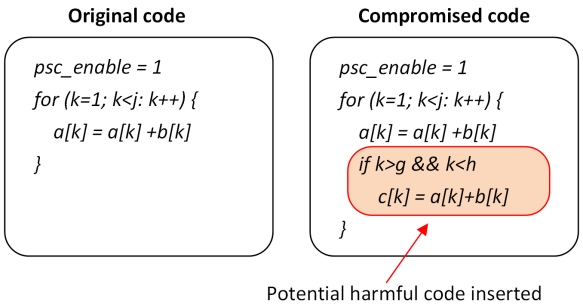


Fig. 6: Microcontroller programs to emulate intact and compromised scenarios

B. Design and simulation of PRIDES generation circuit

In this study, the proposed PRIDES generation circuit is implemented with a 90 nm CMOS technology. The size of the transistors used in the first two stages are listed in Table I. Large channel lengths are selected for M3-4 and M7-8 in order to increase transistor output resistance, which results in sharp transition (higher gain) in the region around gate threshold V_M in the inverter voltage transfer curve. The minimum channel length (100 nm) is used for M2 and M6 to reduce their on-resistance when conducting. The size of M1 and M5 are optimized to compensate the channel charge injection by M2 and M6 when they are turning off. The inverters comprised of M9-10 and M11-12 are digital gates and their transistor sizes are not critical. The sampling capacitors C1 and C2 are selected as 100 fF.

TABLE I: MOS transistor size

MOSFET	Width (nm)	Length (nm)
M1, M5	120	100
M2, M6	1200	100
M3, M7	3600	300
M4, M8	1800	300

The designed circuit is simulated using Cadence Spectre tool. Figure 7 shows a snapshot of the waveforms obtained from

simulation. The waveform in the top panel is the power trace data collected from the hardware experiment. The clock signal is displayed in the middle panel and the PRIDES circuit output is plotted in the bottom panel. It shows the PRIDES outputs accurately characterize the rising and descending patterns of the power trace. Circuit simulations were conducted for the 200 collected power traces and the obtained PRIDES bit streams are saved for cross correlation analysis.

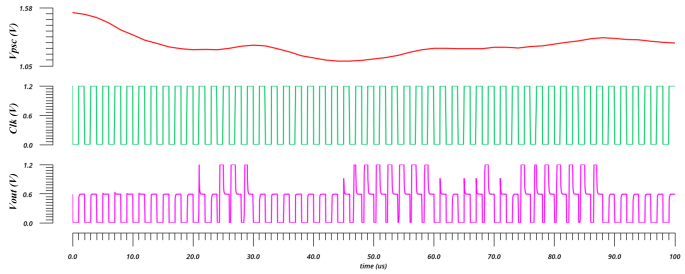


Fig. 7: Simulation result of PRIDES generation circuit from Cadence

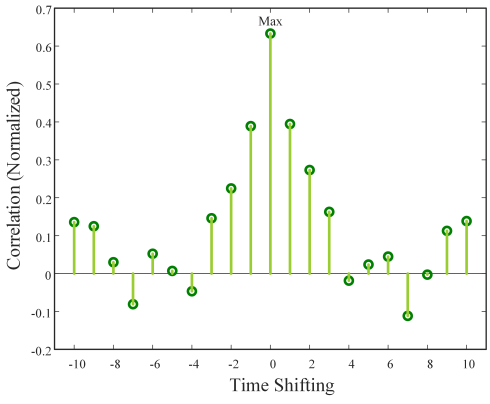
C. PRIDES analysis results

This section presents the performance evaluation of the proposed PRIDES signature in detecting compromised operations. Figure 8(a) provides an example illustrating how the cross correlation values fluctuate with the time shifting operation. In this example, the PRIDES is for the execution of the intact code. It shows that the maximum correlation is achieved at position 0, indicating that the timing of PRIDES capturing was perfectly aligned with the timing of golden signature. However, in other cases the PRIDES and golden signatures may not be perfectly aligned and hence the correlation peak may not always occur at position 0. For the PRIDES associated with the execution of the intact code on MCU1, the positions that lead to the maximum correlation values are shown in Figure 8(b).

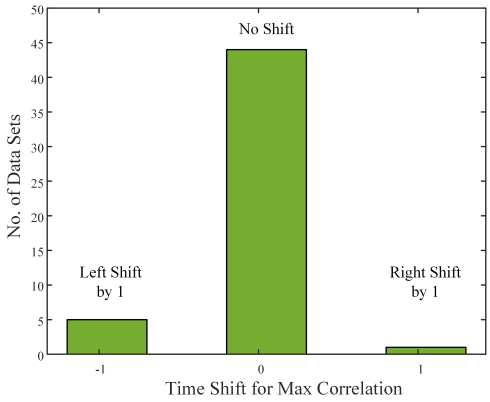
The histogram of the maximum correlations for the 100 PRIDES obtained from MCU1 is shown in Figure 9. Clearly, the values are distributed into two distinct groups. The left group is constituted by PRIDES from the execution of the compromised code and the right group contains the PRIDES associated with the execution of the intact code. There is a very large gap, referred to as the *detection margin (DM)*, between the two groups. With using ζ^I_{LB} and ζ^C_{UB} to denote the correlation lower bound of the intact operations and the correlation upper bound of the compromised operations, the detection margin can be defined as $DM = \zeta^I_{LB} - \zeta^C_{UB}$ as shown in Figure 9.

In the experiment, the clock frequency of the PRIDES generation circuit was varied from 100 kHz to 500 kHz to study the impact of sampling rate on the proposed method. The detection margins at different sampling rates are plotted in Figure 10. It shows the proposed method can tolerate relatively low sampling rates. In general, smaller sampling rates lead to more compact PRIDES.

Despite golden signature $\mathcal{S}$ was obtained using MCU1, it is also suited for detecting the compromised operation on MCU2.



(a)



(b)

Fig. 8: (a) Correlation values at different time shifting position, (b) Distribution of time shifting positions leading to the correlation peak

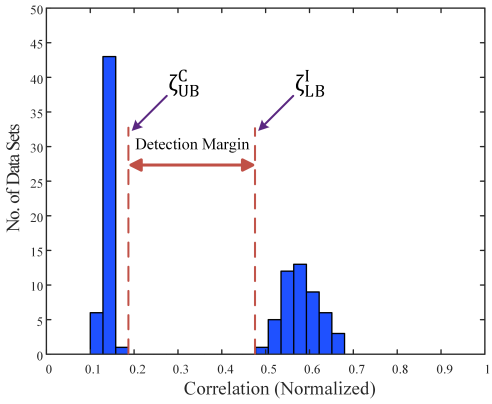


Fig. 9: Detection margin in PRIDES analysis

Table II summarizes the detection margins, ζ^I_{LB}, and ζ^C_{UB} for the PRIDES obtained from different devices. Compared to MCU1, the detection margin for MCU2 is slightly reduced. However, it is still large enough to distinctly separate the PRIDES associated with intact and compromised operations. These results validate the practicality of the proposed method.

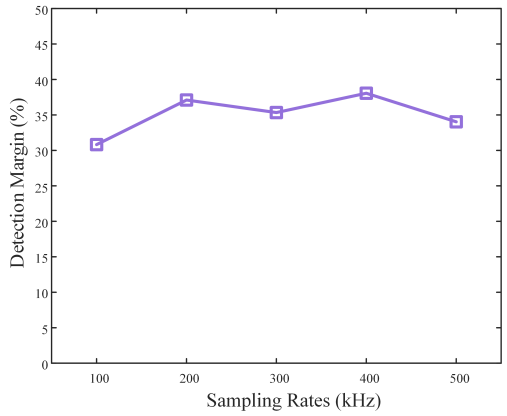


Fig. 10: Detection margin for different sampling rates

TABLE II: Correlation between golden signature $\mathcal{S}$ and PRIDES from different devices

Detection Parameters (Normalized)	**MCU 1**	**MCU 2**
ζ_{LB}^{I}	0.5018	0.4972
ζ_{UB}^{C}	0.1615	0.2068
$Detection\ Margin\ (\%)$	34.03	29.04

V. CONCLUSION

In this paper, we have presented a digital signature, PRIDES, to characterize the rising and descending patterns of device power dissipation. A novel PRIDES generation circuit and a PRIDES-based methodology for abnormality detection are also presented. The effectiveness of the proposed methodology was demonstrated with data captured from hardware experiments. The PRIDES is much more compact compared to conventional power trace data and can be generated using simple circuits. Hence, the proposed method incurs small hardware overhead and is computationally light, making it very suitable for IoT applications.

ACKNOWLEDGMENT

This work is partially supported by the National Science Foundation under Grant No. 2231623. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] Wójcicki, Krzysztof, et al. “Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities—A Review.” Energies 15.5 (2022): 1806.

[2] Al-Kahtani, Mohammad S., Faheem Khan, and Whangbo Taekeun. “Application of internet of things and sensors in healthcare.” Sensors 22.15 (2022): 5738.

[3] Farooq, Muhammad Shoaib, et al. “A survey on the role of iot in agriculture for the implementation of smart livestock environment.” IEEE Access 10 (2022): 9483-9505.

[4] Goudarzi, Arman, et al. “A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook.” Energies 15.19 (2022): 6984.

[5] Khayyam, H., Javadi, B., Jalili, M., Jazar, R.N. (2020). “Artificial Intelligence and Internet of Things for Autonomous Vehicles.” In: Jazar, R., Dai, L. (eds) Nonlinear Approaches in Engineering Applications. Springer, Cham.

[6] Satheeskanth, N., et al. “IoT-based integrated smart home automation system.” Ubiquitous Intelligent Systems: Proceedings of ICUIS 2021. Springer Singapore, 2022.

[7] Internet of Things [IOT] Market Size, Share & Growth by 2030. Available at: https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307 (Accessed: April 27, 2023).

[8] MacBride, E. (2023) The Dark Web’s criminal minds see internet of things as Next Big Hacking Prize, CNBC. Available at: https://www.cnbc.com/2023/01/09/the-dark-webs-criminal-minds-see-iot-as-the-next-big-hacking-prize.html (Accessed: April 27, 2023).

[9] Alaba, Fadele Ayotunde, et al. “Internet of Things security: A survey.” Journal of Network and Computer Applications 88 (2017): 10-28.

[10] Hassan, Wan Haslina. “Current research on Internet of Things (IoT) security: A survey.” Computer networks 148 (2019): 283-294.

[11] Sarker, Iqbal H., et al. “Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions.” Mobile Networks and Applications (2022): 1-17.

[12] Standaert, FX. (2010), “Introduction to Side-Channel Attacks.” In: Verbauwhede, I. (eds) Secure Integrated Circuits and Systems. Integrated Circuits and Systems. Springer, Boston, MA.

[13] Laughman, C., Lee, K., Cox, R., Shaw, S., Leeb, S., Norford, L., and Armstrong, P., 2003, “Power signature analysis.” IEEE power and energy magazine, 1(2), pp.56-63.

[14] Kocher, P., Jaffe, J., Jun, B., and Rohatgi, P. (2011). “Introduction to differential power analysis.” Journal of Cryptographic Engineering, 1(1), 5-27.

[15] Randolph, M., and Diehl, W. (2020). “Power side-channel attack analysis: A review of 20 years of study for the layman.” Cryptography, 4(2), 15.

[16] Agrawal, D., Rao, J.R., Rohatgi, P. (2003), “Multi-channel Attacks.” In: Walter, C.D., Koç, Ç.K., Paar, C. (eds). Cryptographic Hardware and Embedded Systems - CHES 2003,” CHES 2003. Lecture Notes in Computer Science, vol 2779. Springer, Berlin, Heidelberg.

[17] Park, J., and Tyagi, A. (2017), “Using Power Clues to Hack IoT Devices: The power side channel provides for instruction-level disassembly.” IEEE Consumer Electronics Magazine, 6(3), 92-102.

[18] Eisenbarth, T., Paar, C., Weghenkel, B., Gavrilova, M. L., Tan, C. J. K., and Moreno, E. D. (2010), “In Building a Side Channel Based Disassembler.” Transactions on computational science x, (pp. 78-99). Berlin: Springer-Verlag.

[19] Msgna, M., Markantonakis, K., and Mayes, K. (2014, May), “Precise instruction-level side channel profiling of embedded processors.” In International conference on information security practice and experience (pp. 129-143). Springer, Cham.

[20] Strobel, D., Bache, F., Oswald, D., Schellenberg, F., and Paar, C. (2015, March), “Scandalee: a side-channel-based disassembler using local electromagnetic emanations.” In 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 139-144). IEEE.

[21] Bridges, Robert, et al. “Towards malware detection via cpu power consumption: Data collection design and analytics.” 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom). IEEE, 2018.

[22] Jimenez, Jarilyn Hernandez, and Katerina Goseva-Popstojanova. “Malware detection using power consumption and network traffic data.” 2019 2nd International Conference on Data Intelligence and Security (ICDIS). IEEE, 2019.

[23] Shende, Roshni, and Dayanand D. Ambawade. “A side channel based power analysis technique for hardware trojan detection using statistical learning approach.” 2016 thirteenth international conference on wireless and optical communications networks (WOCN). IEEE, 2016.

[24] Wang, Xiaoxiao, et al. “Hardware Trojan detection and isolation using current integration and localized current analysis.” 2008 IEEE international symposium on defect and fault tolerance of VLSI systems. IEEE, 2008.