# POSTER: Post-Quantum Cipher Power Analysis in Lightweight Devices

Kathryn Hines
University of Colorado Colorado Springs, CO, USA
khines2@uccs.edu

Manohar Raavi
University of Colorado Colorado Springs, CO, USA
mraavi@uccs.edu

John-Michael Villenueve
University of Colorado Colorado Springs, CO, USA
jvillene@uccs.edu

Simeon Wuthier
University of Colorado Colorado Springs, CO, USA
swuthier@uccs.edu

Javier Moreno-Colin
University of Washington Tacoma, WA, USA
jmc64@uw.edu

Yan Bai
University of Washington Tacoma, WA, USA
yanb@uw.edu

Sang-Yoon Chang
University of Colorado Colorado Springs, CO, USA
schang2@uccs.edu

## ABSTRACT

Post-quantum ciphers (PQC) provide cryptographic algorithms for public-key ciphers which are computationally secure against the threats from quantum-computing adversaries. Because the devices in mobile computing are limited in hardware and power, we analyze the PQC power overheads. We implement the new NIST PQCs across a range of device platforms to simulate varying resource capabilities, including multiple Raspberry Pis with different memories, a laptop, and a desktop computer. We compare the power measurements with the idle cases as our baseline and show the PQCs consume considerable power. Our results show that PQC ciphers can be feasible in the resource-constrained devices (simulated with varying Raspbery Pis in our case); while PQCs consume greater power than the classical cipher of RSA for laptop and desktop, they consume comparable power for the Raspberry Pis.

## CCS CONCEPTS

• **Security and privacy → Digital signatures**; **Cryptography**.

## KEYWORDS

Post-Quantum Cryptography, Power Measurements, Internet of Things, Wireless Devices, Lightweight Devices, Raspberry Pi

**ACM Reference Format:**
Kathryn Hines, Manohar Raavi, John-Michael Villenueve, Simeon Wuthier, Javier Moreno-Colin, Yan Bai, and Sang-Yoon Chang. 2022. POSTER: Post-Quantum Cipher Power Analysis in Lightweight Devices. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22), May 16–19, 2022, San Antonio, TX, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3507657.3529652

*ACM WiSec '22, May 16–19, 2022, San Antonio, Texas*

ACM ISBN 978-1-4503-9216-7/22/05.
https://doi.org/10.1145/3507657.3529652

## 1 INTRODUCTION

With the rise of quantum computing and its ability to solve the classically difficult problems within polynomial time, the classical ciphers such as RSA [13] and ECDSA [3] are expected to become vulnerable when quantum computers become practical. Post-quantum ciphers, or PQCs, are cryptographic algorithms that are designed to be secure against these quantum attacks. This is achieved by using methods such as Fast-Fourier Lattice-based mathematical algorithms, which are assumed to be difficult mathematical problems that quantum computers cannot solve in polynomial time. These ciphers are also known to be, in general, more computationally intensive, due to their large key sizes and large libraries.

With the rise of Internet of Things (IoT) devices, security is becoming ever more of a challenge. Mobile computing devices including the lightweight devices need transition to the use of the PQC standards which are known to induce computational and memory overheads. Implementing these encryption algorithms on IoT devices would help protect privacy and security in a world of increasing technology. However, it is also important to understand the power consumption of PQCs before transitioning to lightweight devices with limited power resources. In comparison to high-powered machines such as desktops or server machines, these devices have extremely limited CPU power and memory resources. This includes smaller devices like smart watches, where resources are constrained and affects the overall performance of a device. In this paper, we study the feasibility and overheads of PQCs to establish their power requirements on resource constrained devices. Our work focuses on analyzing the power consumption of NIST PQCs and RSA-4096 on 5 different platforms (Section 3). All the PQCs are Round 3 finalists in the National Institute of Standards and Technology's (NIST) post-quantum cipher standardization competition [10].

## 2 BACKGROUND AND RELATED WORK

**PQC** We focus on NIST standardization, considering their global impact as demonstrated by standardization of DES in 1970s and AES in 1990s and their very wide use even in current days. The current NIST algorithms for digital signatures [10] include Dilithium

| Machine | RAM(GB) | Processor | OS |
|---|---|---|---|
| Raspberry Pi 3 | 1 | Quad core Cortex-A53 ARM 1.2 GHz | Raspbian GNU/Linux 11 (bullseye) |
| Raspberry Pi 3 | 2 | Quad core Cortex-A72 (ARM v8) SoC 1.5GHz | Raspbian GNU/Linux 11 (bullseye) |
| Raspberry Pi 4 | 4 | Quad core Cortex-A72 (ARM v8) SoC 1.5GHz | Raspbian GNU/Linux 11 (bullseye) |
| Laptop | 16 | Quad core AMD Ryzen 7 3750H 2.3GHz | Ubuntu 18.04.6 LTS |
| Desktop | 64 | 24-Core AMD Ryzen Threadripper 3960X 3.8GHz | Ubuntu 18.04.6 LTS |

**Table 1: Machine Specifications of Our Testing Platforms**

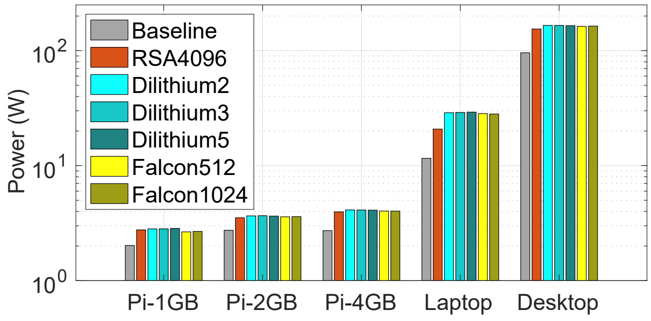

**Figure 1: Power measurements across platforms with varying resource capabilities including three Raspberry Pis, a laptop, and a desktop. The power consumption measurements are for the verification of digital signature-based authentication. The results include the idle baseline and the RSA (classical as opposed to post-quantum) for references for comparison.**

(Dilithium2, Dilithium3 & Dilithium5) and Falcon (Falcon-512 & Falcon-1024) family parameter sets of different key sizes and security strengths. Previous literature analyzes the computational and memory overheads of PQCs [11, 12], the power consumption of Raspberry Pis and other lightweight devices [1, 2, 8], and the power overheads when PQC algorithms are implemented on specific hardware modules [14, 15, 17]. Our work differs from these previous works by comparing the power consumption of the most recent PQCs (the current Round 3 ciphers in NIST) across a range of different platforms including multiple Raspberry Pis with different resources, a laptop, and a desktop.

**Power Importance for Wireless and Mobile Devices** Computing and networking consume electrical power. The power resource is especially invaluable for the wireless/mobile devices operating on batteries with limited energy supply. Highlighting such importance are RFID using backscattering (as opposed to its own generated signals) for communications leveraging the other's signal/power, harvesting energy from the networking signals (e.g., RF signals) [7, 19], the advancement and optimization of wireless charging [4, 9, 20], or protecting the energy availability against the energy-targeting denial-of-service threats [5, 7]. Our work is also motivated by the importance of the power resources for wireless/mobile devices but focus on studying the power feasibility/overheads of the PQC ciphers (orthogonal to these previous research).

## 3 EXPERIMENTAL DESIGN AND SETUP

We run the algorithms specified in Section 2, on three Raspberry Pi boards, having 1GB, 2GB, and 4GB of RAM. We compare the power consumption on the resource-constrained devices against two other platforms, a laptop and a desktop computer, with 16GB and 64GB of RAM, respectively. We specify the processor and operating system information in Table 1.

The power consumption overheads depend on the implementations/libraries as well as the computing platforms. In order to provide analyses results and insights which are robust across the different implementations and platforms, we take a differential approach by introducing references for our power measurements and focus on the comparison with those references. In addition to the power measurements of the PQC ciphers, we introduce two references. First, each machine has a *baseline* power consumption, as defined when the processor is idle. This measurement is taken while each device is in its lowest natural state of CPU usage, powered on and running with no user programs. Bluetooth and Wi-Fi are switched off. Second, we include a classical cipher, RSA-4096 (RSA), to enable a comparison between PQC vs. classical.

We use a wall outlet power meter which measures voltage (V), current (I), power (W), and power factor (PR10-E Power Recorder, manufactured by Shenzhen Zhurui Technology Company, Ltd.). Using the OpenSSL library for RSA, and the Open Quantum Safe [18] library for the PQCs, we isolate and run each cipher serially, looping through the verify function for a specified amount of time. Concurrently, we record the wattage displayed to measure its power consumption.

## 4 POWER MEASUREMENTS RESULTS AND PERFORMANCE ANALYSIS

Figure 1 shows the power consumption of the PQC verification across different platforms detailed in Section 3. For baseline power measurements, the Raspberry Pis power consumption is 2.02 - 2.79 W, depending on the memory, while those of laptop and desktop are 11.58 W and 95.9 W, respectively. The desktop, laptop, and 4GB-Pi baseline powers are 4,642.10%, 472.46%, and 34.66% higher than the baseline power of the 1GB-Pi.

We compare the power draw of the ciphers against our first reference, the baseline power of the machines. RSA power consumption on the 1GB-Pi is 36.61% higher than the baseline. With Dilithium5 and Falcon-1024, the highest security version of Dilithium and Falcon families, the power consumption is 40.67% and 32.51% higher than the baseline, respectively. Dilithium5 is 152.20% and 72.00% higher than the baseline on the laptop and desktop, respectively, with Falcon-1024 being 142.91% and 70.56% higher.

We also analyze the difference between the PQCs and our second reference, the classical cipher of RSA. Dilithium5 power draw is 2.97% higher than RSA on the 1GB-Pi, and Falcon is 3.00% lower. This behavior is similar across all three Raspberry Pis, with RSA being very similar to the PQC power draw. According to our results, this indicates that RSA does not have a significantly greater power draw than the PQCs on the Raspberry Pis. This could be due to the key length of the RSA cipher used, 4096 bits, and the OpenSSL library. This key length was used due to its common application in communications; it was desired to create a realistic environment. In comparison, the public and secret key lengths of Dilithium 5 are 2592B and 4864B, respectively, while Falcon-1024 has public and secret key lengths of 1793B and 2305B, respectively [16]. This difference could also be due to the difference between the OpenSSL and liboqs libraries. OpenSSL, which we use to implement RSA, is known to be a large library.

However, on the laptop and the desktop, the power draw of PQCs is noticeably higher than RSA's, with Dilithium5 being 40.54% and 6.89% higher, respectively, and Falcon-1024 being 35.22% and 6.00% higher. Such behavior is expected because PQCs are known to be more computationally demanding and expected to require more hardware resources. The discrepancy between the Raspberry Pis and the laptop could be due to differences in the way the libraries are implemented on different hardware.

One more takeaway of our analysis is related to the question of the practicality of running PQCs on resource-constrained devices. We see that the PQCs only raise the power consumption by a maximum of 40.67% on the 1GB-Pi (the most resource-constrained among our tested platforms), in comparison to the baseline. This, coupled with future work on CPU usage and time demands of PQCs, could indicate the feasibility of running these PQCs on resource-constrained devices.

## 5 CONCLUSION AND FUTURE WORK

In this paper, we perform a power analysis of post-quantum ciphers on resource-constrained devices. We accomplish this by running five of NIST's PQC Standardization Round 3 competitors on three Raspberry Pis with different resource capabilities and measuring the power draw. Our analysis also includes two devices with essentially unlimited resources, a laptop and a desktop. We include in our analysis the comparison with the pre-quantum cipher of RSA. We analyze these results and demonstrate that it is quite feasible to run the post-quantum ciphers on a resource-constrained device with as low as 1GB of RAM. Power consumption is not be the only parameter of concern while considering feasibility. Other important aspects to study include the CPU usage and the length of time required to run each cipher.

There is a need for post-quantum security on other IoT devices that are more limited on resources, such as pacemakers or smart watches, due to the extremely small processors and RAM. In this analysis, we implement the ciphers with their respective large libraries. With an even smaller device, it will be difficult or impossible to implement the liboqs library, especially on a pacemaker whose RAM size is 10KB [6] and whose operating system does not support libraries. A more compact implementation of the PQCs would be needed for resource constrained IoT devices to secure the data in the upcoming quantum era.

## ACKNOWLEDGEMENT

This work was supported in part by National Science Foundation under Grant No. 1922410 and Grant No. 1921576.

## REFERENCES

[1] Girish Bekaroo and Aditya Santokhee. 2016. Power consumption of the Raspberry Pi: A comparative analysis. In *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*. IEEE, 361–366.

[2] Kevin Bürstinghaus-Steinbach, Christoph Krauß, Ruben Niederhagen, and Michael Schneider. 2020. Post-quantum tls on embedded systems: Integrating and evaluating kyber and sphincs+ with mbed tls. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. 841–852.

[3] William J Caelli, Edward P Dawson, and Scott A Rea. 1999. PKI, elliptic curve cryptography, and digital signatures. *Computers & Security* 18, 1 (1999), 47–66.

[4] Sang-Yoon Chang, Sristi Lakshmi Sravana Kumar, and Yih-Chun Hu. 2017. Cognitive Wireless Charger: Sensing-Based Real-Time Frequency Control For Near-Field Wireless Charging. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. 2302–2307. https://doi.org/10.1109/ICDCS.2017.260

[5] Sang-Yoon Chang, Sristi Lakshmi Sravana Kumar, Bao Anh N. Tran, Sreejaya Viswanathan, Younghee Park, and Yih-Chun Hu. 2017. Power-Positive Networking Using Wireless Charging: Protecting Energy against Battery Exhaustion Attacks. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Boston, Massachusetts) *(WiSec '17)*. Association for Computing Machinery, New York, NY, USA, 52–57. https://doi.org/10.1145/3098243.3098265

[6] Santosh D Chede and Kishore D Kulat. 2008. Design Overview Of Processor Based Implantable Pacemaker. *J. Comput.* 3, 8 (2008), 49–57.

[7] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. 2008. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*. 129–142. https://doi.org/10.1109/SP.2008.31

[8] Fabian Kaup, Philip Gottschling, and David Hausheer. 2014. PowerPi: Measuring and modeling the power consumption of the Raspberry Pi. In *39th Annual IEEE Conference on Local Computer Networks*. IEEE, 236–243.

[9] Adelina Madhja, Sotiris Nikoletseas, and Alexandros A. Voudouris. 2019. Adaptive wireless power transfer in mobile ad hoc networks. *Computer Networks* 152 (2019), 87–97. https://doi.org/10.1016/j.comnet.2019.02.004

[10] National Institute of Standards and Technology. 2017. *NIST Status Update on the 3rd Round.* Retrieved March 16, 2022 from https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf

[11] Manohar Raavi, Pranav Chandramouli, Simeon Wuthier, Xiaobo Zhou, and Sang-Yoon Chang. 2021. Performance Characterization of Post-Quantum Digital Certificates. In *2021 International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 1–9.

[12] Manohar Raavi, Simeon Wuthier, Pranav Chandramouli, Yaroslav Balytskyi, Xiaobo Zhou, and Sang-Yoon Chang. 2021. Security comparisons and performance analyses of post-quantum signature algorithms. In *International Conference on Applied Cryptography and Network Security*. Springer, 424–447.

[13] Ronald L Rivest, Adi Shamir, and Leonard Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21, 2 (1978), 120–126.

[14] Crystal Andrea Roma, Chi-En Amy Tai, and M Anwar Hasan. 2021. Energy Efficiency Analysis of Post-Quantum Cryptographic Algorithms. *IEEE Access* 9 (2021), 71295–71317.

[15] Markku-Juhani O Saarinen. 2020. Mobile energy requirements of the upcoming NIST post-quantum cryptography standards. In *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. IEEE, 23–30.

[16] Open Quantum Safe. 2022. *Algorithms in liboqs.* https://openquantumsafe.org/liboqs/algorithms/

[17] Maximilian Schöffel, Frederik Lauer, Carl C Rheinländer, and Norbert Wehn. 2021. On the Energy Costs of Post-Quantum KEMs in TLS-based Low-Power Secure IoT. In *Proceedings of the International Conference on Internet-of-Things Design and Implementation*. 158–168.

[18] Douglas Stebila and Michele Mosca. 2017. Post-quantum Key Exchange for the Internet and the Open Quantum Safe Project. In *Selected Areas in Cryptography – SAC 2016*, Roberto Avanzi and Howard Heys (Eds.). Springer International Publishing, Cham, 14–37.

[19] Vamsi Talla, Bryce Kellogg, Benjamin Ransford, Saman Naderiparizi, Shyamnath Gollakota, and Joshua R. Smith. 2015. Powering the next Billion Devices with Wi-Fi. In *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies* (Heidelberg, Germany) *(CoNEXT '15)*. Association for Computing Machinery, New York, NY, USA, Article 4, 13 pages. https://doi.org/10.1145/2716281.2836089

[20] N. Tesla. 1914. Apparatus for transmitting electrical energy. http://www.google.com/patents/US1119732 US Patent 1,119,732.