12-1-2020

Cybersecurity of the Artificial Pancreas

D. J. Cooke
Boise State University

Andres Guzman
Boise State University

Robert Kinney
Boise State University

Christine Patterson
Boise State University

Josh Stone
Boise State University

Cybersecurity of the Artificial Pancreas

Daniel Cooke, Andres Guzman, Robert Kinney, Christine Patterson, Josh Stone

BOISE STATE UNIVERSITY

Measuring Power Consumption of Cryptographic Algorithms

INTRODUCTION

We live in a world of cyber-enabled, wireless devices that enhance many aspects of life, including treatment of diabetes. Type I Diabetes is a chronic autoimmune disorder characterized by the destruction of pancreatic B-cells and subsequent deficiency of insulin - a crucial hormone in the regulation of blood glucose levels. Implantable Medical Devices (IMD) are shrinking in physical size which limits their memory, power, and processing capacity resulting in the unsecure transmission of data. The National Institute of Standards and Technology (NIST) has called for encryption algorithms to be considered as the lightweight cryptographic standard to combat these vulnerabilities. In this poster, we analyze the power consumption of a lightweight encryption candidate for use in a continuous glucose monitor.

CONTINUOUS GLUCOSE MONITOR (CGM)

- Transmits blood glucose levels from the interstitial fluid every 5 minutes
- Bluetooth Low Energy communication
- Limited battery, memory, and computing resources
- Sensors last ~10 days, Transmitters last ~90 days

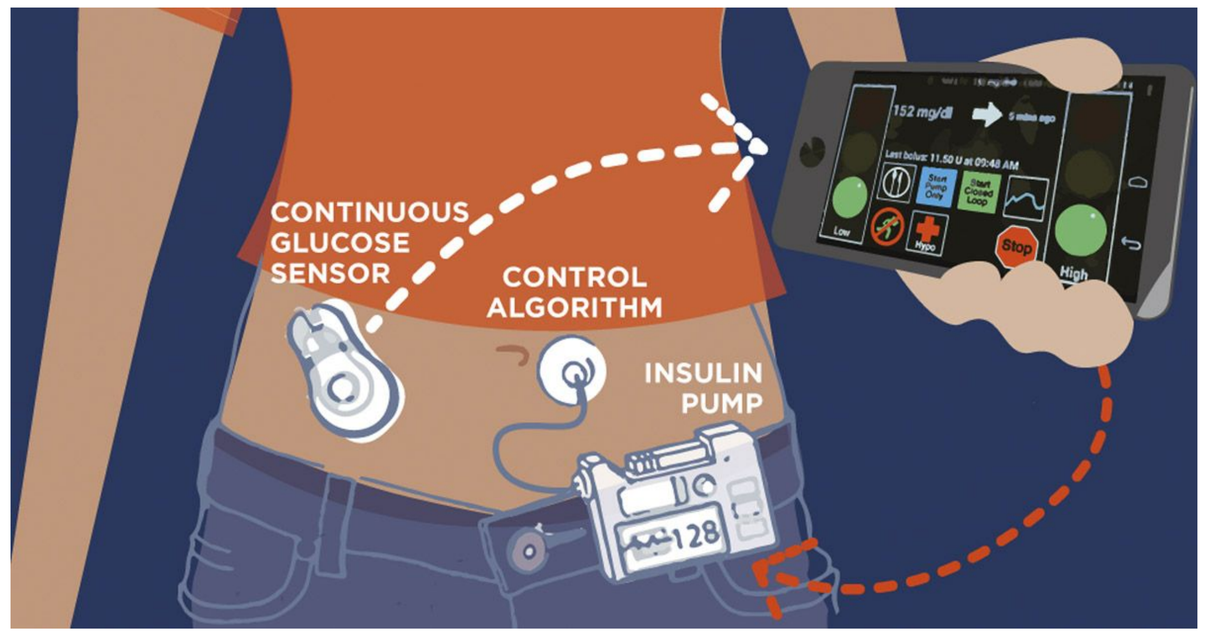

Figure 1: The loop of diabetes treatment using a CGM, smartphone, and insulin pump

SECURITY GOALS

1) Cryptographic strength should be equal to or comparable to round two candidates in the NIST Lightweight Crypto Standardization project.
2) The power usage of the device cannot exceed the max draw of the battery during encryption or regular usage
3) The battery lifespan of a device using lightweight encryption should be comparable to the device's default power consumption.

ForkAE

ForkAE is a lightweight authenticated encryption scheme optimized for short messages. Fork is a 2nd-round candidate for the NIST Lightweight Cryptographic Standard. In [1], it is claimed that Fork is an appropriate cryptosystem for resource constrained devices including IMDs. Figure 2 depicts the mathematical structure of one round of Fork.

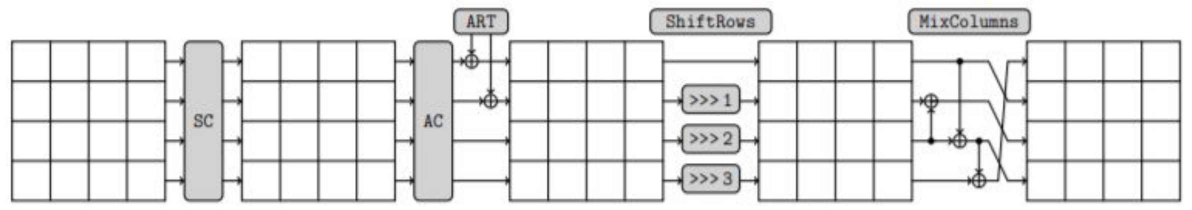

Figure 2: Structure of one round of Fork [2]

METHODS

We used an oscilloscope to record the current and voltage consumed by a Raspberry Pi 4B that computes a ciphertext of ForkSkinny-64-192 every .1 seconds for 10 seconds. The voltage and current were used to analyze power consumption of the encryption.

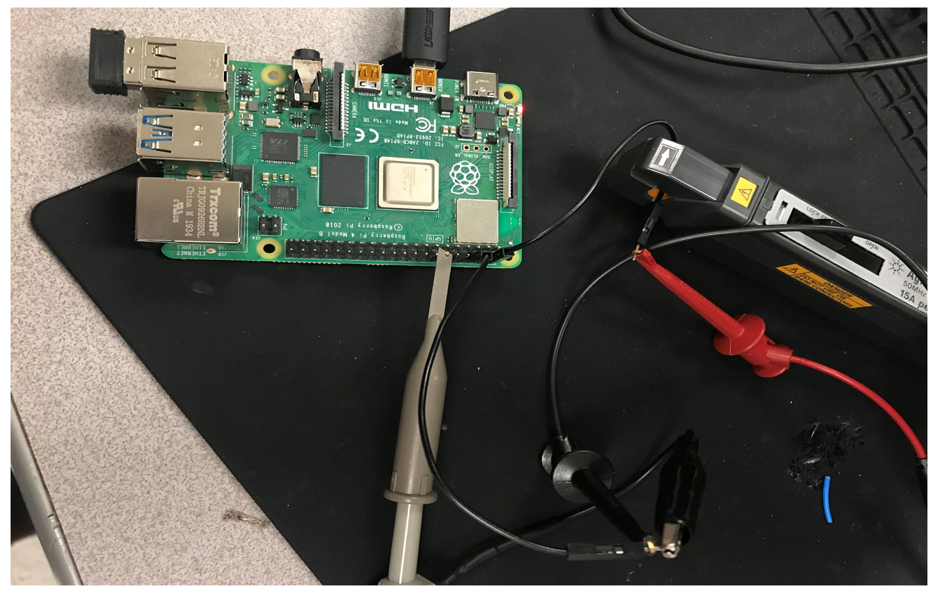

Figure 3: Raspberry Pi 4 configured for experimentation.

DATA

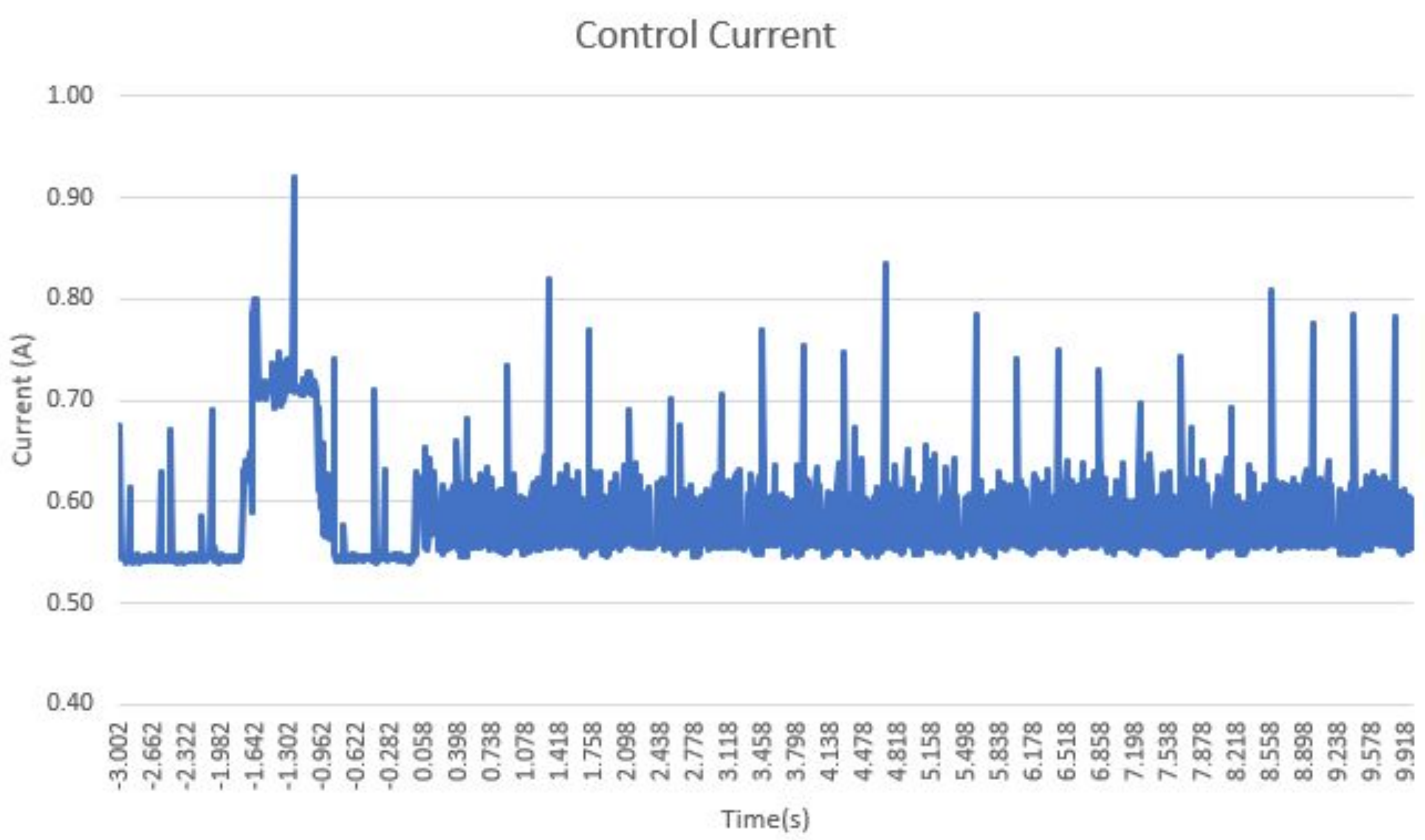

Figure 4: Current draw of the Raspberry Pi without encryption

The graph above shows the current draw of the Raspberry Pi without computing ciphertexts. The variation in current indicates lots of interference from the needs of the operating system.

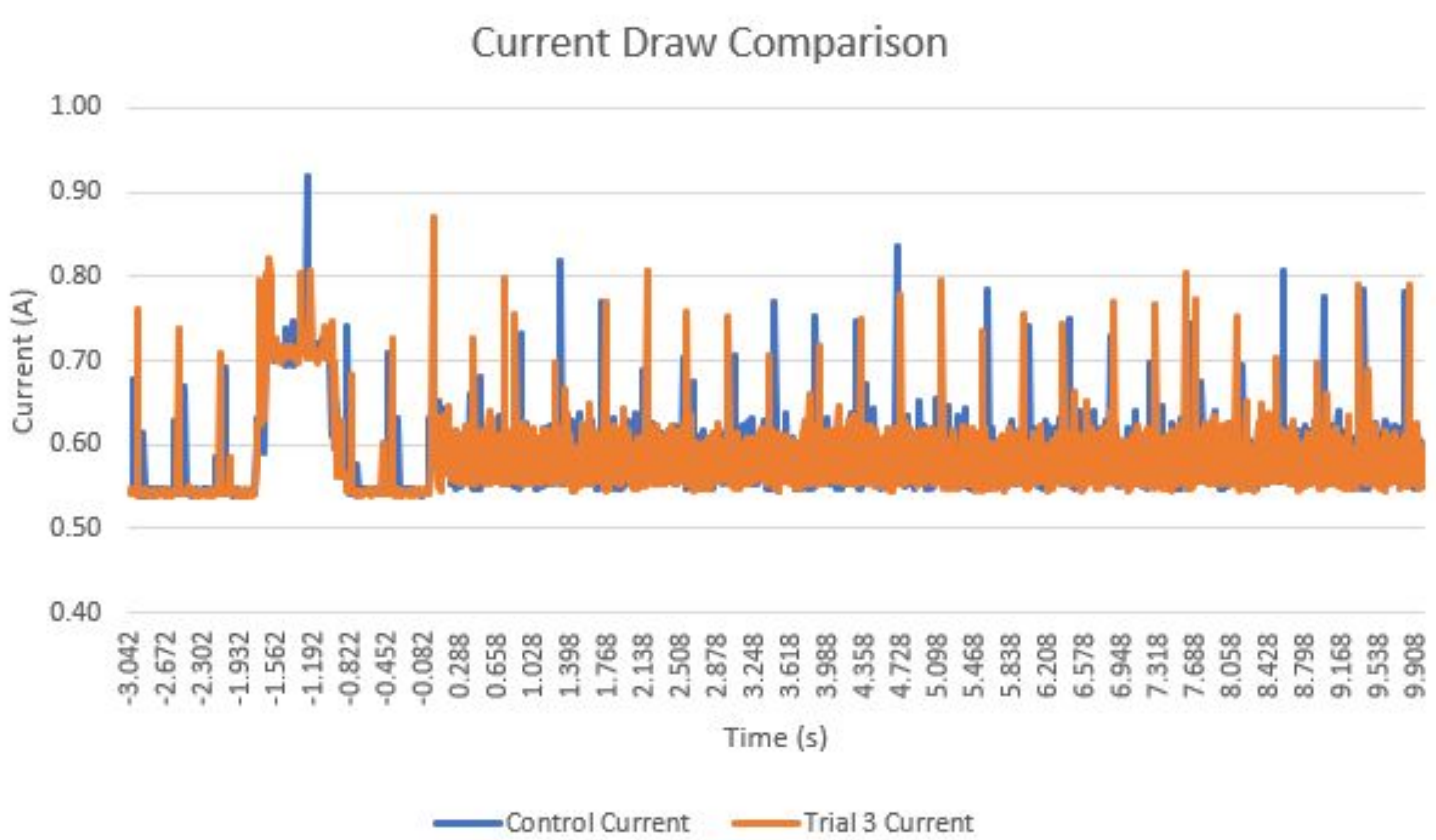

Figure 5: An overlay of the current draw of the Raspberry Pi while computing ciphertexts of ForkAE compared to the control trial.

This graph is the current draw of the Pi while computing ciphertexts (orange) over the control trial from Figure 4. We see little variation between the trials indicating that the encryption has minimal power consumption.

CONCLUSION

In the test runs we performed we were able to perform encryption without exceeding the thresholds measured in the control run. Our data sets indicate a pattern that matches our expectations, but there is too much interference from the operating system to quantify the power consumption. The similarity in data between trials has a strong indication that the battery life of a CGM with ForkAE would be comparable to the device's lifespan with default power consumption.

FUTURE WORK

- Perform a similar test on hardware that is resource constrained for a more accurate test environment
- Compare the resource consumption of ForkAE to other lightweight cryptographic algorithms and AES
- Design a simplified version of ForkAE over GF(5^2) in a 2x2 matrix to convert the block size to 100 bits

REFERENCES

[1]Andreeva E. et al., "ForkAE: Lightweight AEAD Submission to NIST", *NIST Lightweight Cryptography Standardization*, (2018).
[2]Andreeva, Elena, et al. "Forkcipher: a new primitive for authenticated encryption of very short messages." *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Cham, 2019.

ACKNOWLEDGMENTS

We thank the Boise State College of Innovation and Design for their support of the project as well as our mentors Dr. Liljana Babinkostova, Robert Erbes (Idaho National Lab), Jay Radcliffe (Thermo Fisher Scientific), Dr. Marion Scheepers and Dr. Edoardo Serra. Data was collected with the help of Professor Brian Higgins in the Boise State Electrical Engineering Lab.