4-23-2021

Cybersecurity of the Artificial Pancreas

Daniel Cooke
Boise State University

Christine Patterson
Boise State University

Aparna Sankaran
Boise State University

Cybersecurity of the Artificial Pancreas

Abstract

The Continuous Glucose Monitor (CGM) plays a crucial role in the treatment of Diabetes by wirelessly transmitting glucose measurements as frequently as every 5 minutes to a receiver or smartphone. CGMs are shrinking to enhance patient compatibility, which limits the physical space available for computational resources making them unsuitable for traditional cryptographic schemes. The National Institute of Standards and Technology (NIST) has called for encryption algorithms to be considered for the lightweight cryptographic standard to be used in resource-constrained environments like a CGM. We provide experimental evidence of the resource consumption of a NIST lightweight finalist in comparison to the Advanced Encryption Standard (AES) when implemented onto the same chip used in CGMs.

Cybersecurity of the Artificial Pancreas

Daniel Cooke, Christine Patterson, Aparna Sankaran

BOISE STATE UNIVERSITY

Measuring Resource Consumption of Cryptographic Algorithms

INTRODUCTION

Type I Diabetes is a chronic autoimmune disorder characterized by the destruction of pancreatic 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 computational resources resulting in unencrypted data transmissions. The National Institute of Standards and Technology (NIST) has called for encryption algorithms to be considered as the lightweight cryptographic standard to secure the communication channel. We present experimental evidence of the resources consumed when encrypting short messages in a constrained environment with a lightweight encryption algorithm in comparison to the Advanced Encryption Standard (AES).

CONTINUOUS GLUCOSE MONITOR (CGM)

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

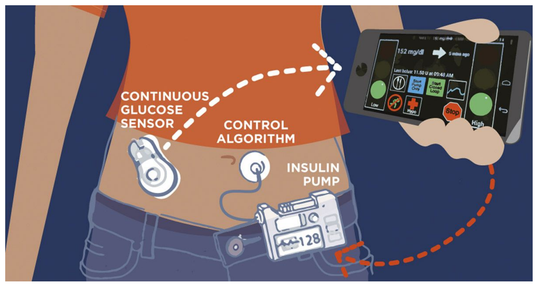

Figure 1: The loop of diabetes treatment using a CGM, smartphone, and insulin pump

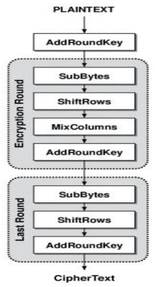

Figure 2: One round of AES [2]

AES

AES [1] is a symmetric block cipher and a current standard for data security. AES is not ideal for IMDs because of the required computational resources to encrypt data. Figure 2 depicts the mathematical structure of one round of AES.

ASCON

Ascon[3] is a family of AEAD algorithms based on the sponge construction. Ascon was a finalist of the CAESAR competition for authenticated ciphers and a current finalist for the NIST lightweight cryptography standardization. It provides resistance against side channel attacks such as the cache and timing attack. Ascon is also likely to be quantum resistant when using a 160-bit key.

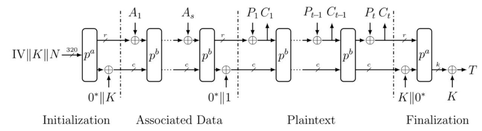

Figure 3: Ascon encryption operation [3]

METHODS

- Implemented AES and Ascon onto Nordic nRF51422 SoC using the nRF51 Development Kit
- Each algorithm encrypted 128-bit message using a 128-bit key with 500ms in between
- Current was measured using Nordic Power Profiler Kit with a supply of 3 volts (equivalent to a CGM)

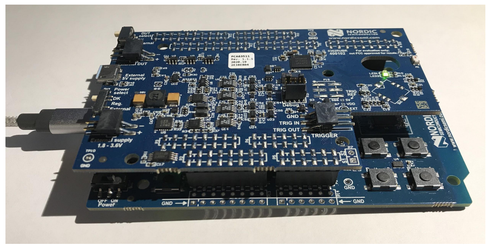

Figure 4: Power Profiler Kit mounted onto the nRF51 Development Kit

DATA

Algorithm	Charge (µC)	Enc Time (ms)	RAM (kB)	ROM (kB)
AES	125.24	26.09	10.9	40.7
Ascon	10.34	2.43	10.2	33.2

Table 1: A comparison of the average values of our experimental results

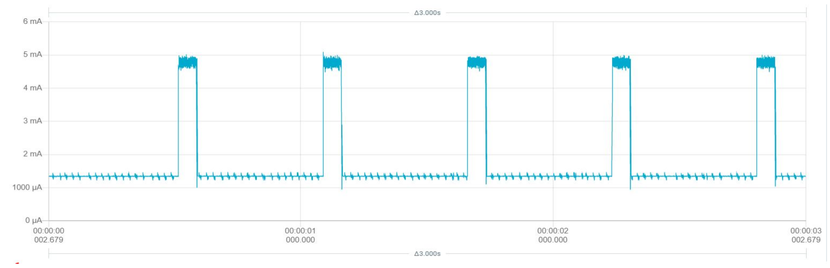

Figure 5: The current draw of encrypting and decrypting with AES every 500ms for 3 seconds

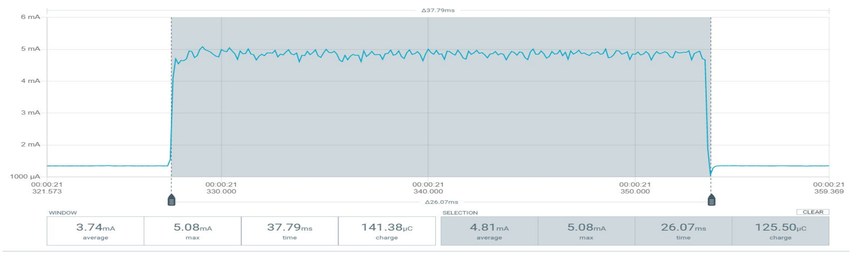

Figure 6: A zoomed-in view of the current draw while encrypting one message with AES

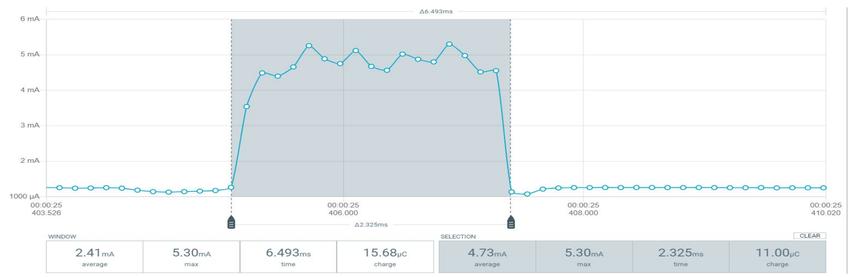

Figure 7: A zoomed-in view of the current draw while encrypting one message with Ascon

CONCLUSION

- AES consumed over 12x more electric charge than Ascon
- Ascon encrypted over 10x faster than AES
- AES required 6.8% more RAM than Ascon
- AES required 43.7% more ROM than Ascon
- The results for current measurements are consistent with those of [2]

FUTURE WORK

- Measure the resource consumption of other NIST lightweight finalists
- Develop a simplified version of a lightweight algorithm using a different finite field and measure the resource consumption
- Experiment with varying inputs to algorithms: message length, associated data, and key

REFERENCES

[1]Daemen, Joan, and Vincent Rijmen. "AES proposal: Rijndael." (1999).

[2]Diehl, William, et al. "Face-off between the CAESAR Lightweight Finalists: ACORN vs. Ascon." *2018 International Conference on Field-Programmable Technology (FPT)*. IEEE, 2018.

[3]Dobraunig, Christoph, et al. "Ascon v1. 2." *Submission to the CAESAR Competition* (2016).

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), and Dr. Marion Scheepers.