# Energy Analysis of Lightweight Encryption Algorithms on Smartphone Application for Wireless Body Area Network Communication

Kelsey Clater[1] and Yuncong Ma[2]
Faculty Mentors: Tao Zhang[2]
Affiliation: [1.] Transylvania University, [2.] School of Engineering and Computing Science, NYIT
Emails: krclater18@transy.edu, {yma14,tzhang}@nyit.edu

## ABSTRACT

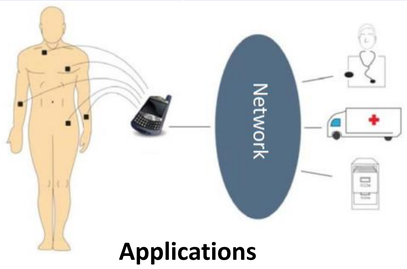
Wireless Body Area Network (WBAN) technology has presented an avenue for increased health care coverage by providing local, constant physiological monitoring. However, WBANs suffer from steep energy limitations. Additionally, as medical information is highly sensitive in nature, ensuring appropriate security while optimizing energy is a major challenge WBANs face. We aim to simulate a WBAN environment, by developing a smartphone application that encrypts mock WBAN sensor data using 4 encryption algorithms. We measured the energy consumption of the application during encryption in order to optimize the tradeoff between security and energy consumption for WBAN purposes. We evaluated the energy impact of each encryption algorithm in conjunction with current cryptanalysis. In conclusion, we recommend an ideal protocol for WBAN security based on our results.

## BACKGROUND

### Wireless Body Area Network (WBAN)

WBAN architecture consists of three layers:

| Layer | Purpose |
|---|---|
| Micro/Nano Wireless Sensors | Collect physiological data. Administer medicine to patient. |
| Mobile Device | Handles data transmission from sensors via Bluetooth and to server via 4G/Wi-Fi. Provides user interface. |
| Back-end Server | Data processing and storage. |




### Applications

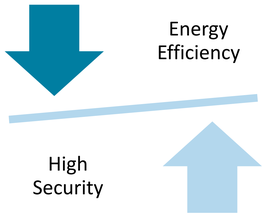
- Medical treatment and diagnosis
- Remote health monitoring
- Personalized care
- Public Safety/Emergency Services
- Military /Uniformed Personnel
- Athlete Training
- Gaming/Entertainment

## PROBLEM & OBJECTIVE

**Energy:** WBAN relies on mobile phone for data transmission. Battery life constrains WBAN functionality.

**Security:** Medical information is very sensitive and must be secure during data transmission

**Objective**: Optimize energy efficiency without compromising security through the implementation of lightweight encryption.




## METHODOLOGY

### Simulated WBAN Environment

Developed an Android Application, **UploadToServer** using Android Studio v2.3.3. The Application is able to encrypt mock WBAN files using 4 different lightweight encryption algorithms: ***Simon, Speck, Sparx and LEA.*** Experiments were carried out on a Nexus 5, Android 6.0.1.

### Energy Measurement

**PowerTutor**, an Android application developed by the University of Michigan is designed to estimate the power consumption of individual applications in milliwatts. PowerTutor records data in an exportable log. PowerTutor was used to measure the power consumption of UploadToSever.

### Data Analysis

DelBello and Kazi Parser, a Matlab program, was used to parse PowerTutor .log file for power consumption of UploadToServer during encryption. Energy was computed using the ***Energy = ∫Power dt*** relationship. The average energy was computed over multiple trials.

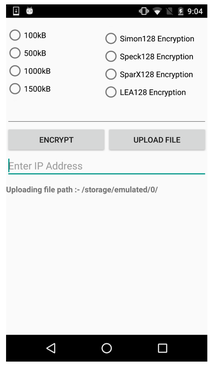



Fig I: Screenshot of UploadToServer

## RESULTS

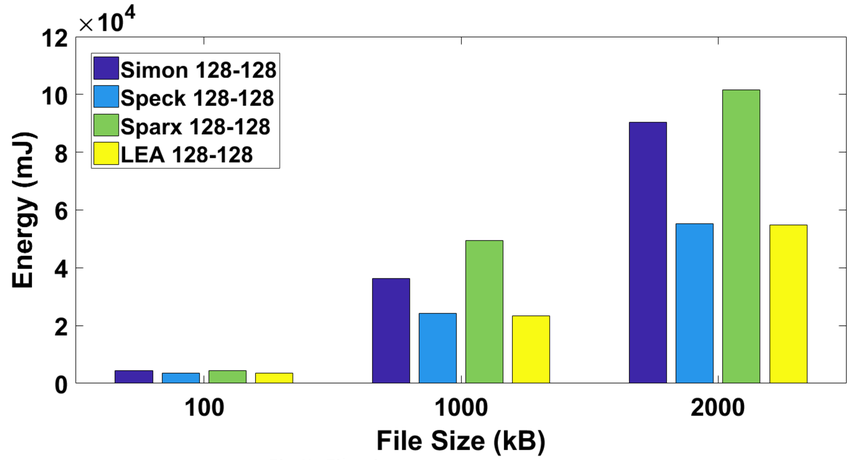



Fig II: File size versus average energy

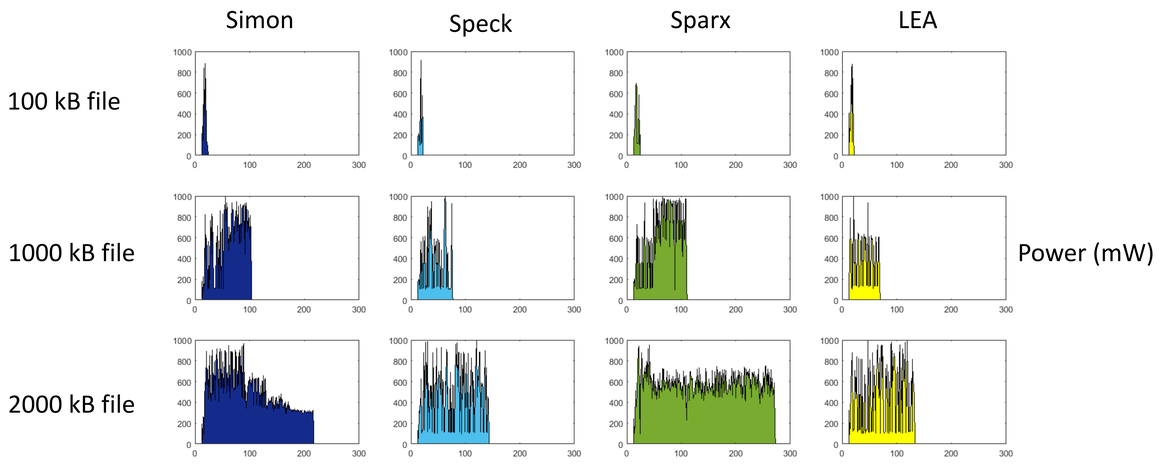



Fig III: Time versus power

## ANALYSIS and DISCUSSIONS

The lightweight encryption classification is used to characterize encryption algorithms that utilizes fewer or simpler computation, less memory resources, and/or has a smaller code size than classical encryption algorithms.

All of the algorithms tested had a block size of 128 bits and a key length of 128 bits. Of the four lightweight encryption algorithms, **LEA** was the most energy efficient; however, Speck consumes only 1.4515% more energy than LEA on average across the 3 file sizes.

LEA, or Lightweight Encryption Algorithm, developed by the Electronics and Telecommunications Institute of Korea, is an ARX block cipher. This means that only modular Addition, bitwise Rotation and bitwise XOR operations are used during the encryption and decryption process. Current cryptanalysis of LEA reveals that it is vulnerable to side-channel differential power analysis attacks. Masking techniques can be used to mitigate this weakness; however, masking increases the overhead of algorithm execution. On the other hand, several differential and rectangle attacks have been made on Speck, with 17 of 32 rounds attacked for Speck128/128.

## CONCLUSIONS

Based on the results of our experiments, we propose that both the LEA and the Speck lightweight encryption algorithms should be considered for ensuring the security of WBAN data during layer 2 – 3 data transmission. Further cryptanalysis is needed for establishing which encryption algorithm has the highest security.

## FUTURE WORK

- Determine optimal latency for WBAN data transmission
- Explore impact of lightweight encryption and data transmission on the battery life of WBAN sensors
- Seek innovative ways to harvest energy for a WBAN from the environment, such as a human's body heat
- Explore Ultra-Wide Band (UWB) transceivers, which feature high data rates and low power consumption
- Further cryptanalysis on LEA encryption algorithm

## REFERENCES

[1] S. Mavassahgi and J. Lipman "Wireless Body Area Networks: A Survery" in *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 3, THIRD QUARTER*, 2014.
[2] C. DelBello and K. Raihan, "Reducing Energy Consumption of Mobile Phones during Data Transmission and Encryption for WBAN Applications." 2014
[3] Power Tutor. A Power Monitor for Android Based Mobile Platforms. http://ziyang.eecs.umich.edu/projects/powertutor/index.html
[4] J. Hong et el "LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors"
[5] R. Beaulieu et al "The SIMON and SPECK Families of Lightweight Block Ciphers" in *Cryptology ePrint Archive, Report 2013/404*, 2013, http://eprint.iacr.org/2013/404
[6] D. Dinu1 et al, "Design Strategies for ARX with Provable Bounds: Sparx and LAX" in *Advances in Cryptology -- ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I,* Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, *484-513*
[7] A. Farzaneh et al, "Differential Cryptanalysis of Round-Reduced Simon and Speck" in *Fast Software Encryption 2014,* London, UK, 2014.
[8] J. Choi and Y. Kim, "An improved LEA block encryption algorithm to prevent side-channel attack in the IoT system," *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, Jeju, 2016, pp. 1-4.

## ACKNOWLEDGEMENT

The project is funded by National Science Foundation Grant No. CNS-1559652 and New York Institute of Technology.