Digital Fingerprints for Low-Cost Platforms using MEMS sensors

Aydin Aysu, Nahid Farhady Ghalaty, Zane Franklin, Moein Pahlavan Yali, Patrick Schaumont
Electrical and Computer Engineering Department
Virginia Tech
Blacksburg, VA, USA
e-mail: { aydinay,farhady, zanef, moein, schaum }@vt.edu

ABSTRACT
With the Internet of Things on the horizon, correct authentication of Things within a population will become one of the major concerns for security. Physical authentication, which is implementing digital fingerprints by utilizing device-unique manufacturing variations, has great potential for achieving this purpose. MEMS sensors that are used in the Internet of Things have not been explored as a source of variation. In this paper, we target a commonly used MEMS sensor, an accelerometer, and utilize its process variations to generate digital fingerprints. This is achieved by measuring the accelerometer's response to an applied electrostatic impulse and its inherent offset values. Our results revealed that MEMS sensors could be used as a source for digital fingerprints for run-time authentication applications.

Keywords
Digital Fingerprints; Physical Authentication; Accelerometer Sensor; RFID; Microcontrollers;

1. INTRODUCTION
The term Internet of Things (IoT) is used to describe a large-scale network of electronic devices that communicates using the Internet protocol. In these networks, to enable a variety of applications, each device would exchange information about itself and its surroundings [1]. Sensors enable these devices to monitor environment parameters such as room temperature, navigation speed or ambient noise. The Internet of Things that is built with these capabilities would eventually become an Internet of Sensors.

The ever-growing market of RFIDs and low-cost microcontrollers introduces new types of platforms that could be used as Things. A popular example of a low-cost, passively powered platform with an integrated sensor is the Wireless Identification and Sensing Platform (WISP), designed by Intel Seattle [2]. In those low-cost, light-weight platforms, MEMS sensors are typically used to interact with the analog world. This interaction could enable many unique applications in a variety of fields from healthcare to cattle management [3].

As we build the Internet of Things, new challenges emerge concerning their security [1]. One of the most significant challenges is being able to correctly identify each of these numerous devices. In certain critical applications, such as weapon condition monitoring for military and law enforcement, the trust that is required from device identifiers is of utmost importance. For example, [4] describes a gunshot event counter using MEMS, which has obvious implications on trust. The secure identification of these numerous devices must be done by means of an authentication protocol.

This research was support in part through NSF Grant 0964680

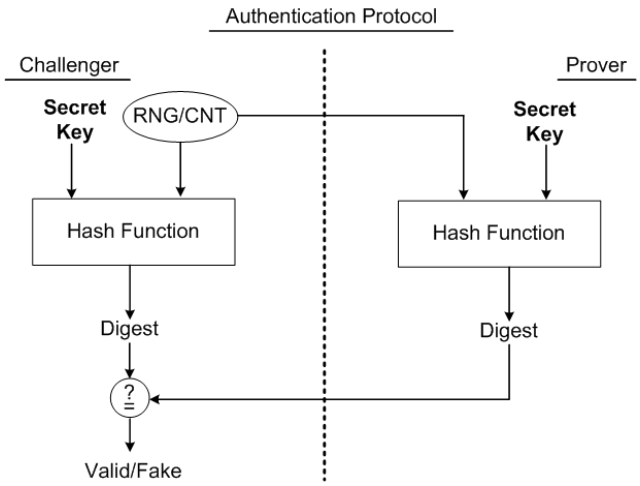

Figure 1. A simple authentication protocol

1.1 Authentication Protocol
Authentication is an important aspect of security. Even when the communication among the included parties is secure against eavesdropping, the system can be compromised if a malicious party is regarded as a trusted one, as it becomes a valid destination of a secret data. Authentication is the first step in many cryptographic protocols that require confidentiality or resource access control. Session key agreement, for example, requires authentication to avoid man-in-the-middle attacks. An authentication protocol is a sequence of steps to achieve this result.

The outline of a simple authentication protocol is given in Fig. 1. The challenger could be the system administrator that tries to verify the identity of a device, and the prover is the device under investigation. The challenger uses a Random Number Generator (RNG) or a counter (CNT) to generate a challenge bitstring and sends it to the prover. The prover combines the input with the secret key and hashes this to generate the message digest. The challenger performs the same operation. The digest value is sent from the prover to the challenger for verification. If the prover's and the challenger's secret keys match, the digests will be the same. Hence, a simple check performed by the challenger verifies the identity of the device and determines whether it is trusted (valid) or not authorized (fake).

1.2 Generating The Secret Key

The scope of this paper is to find a good mechanism to generate the secret key that will be used in the authentication protocol. Biometrics for authentication of individuals are widely adopted in systems where humans are the trusted parties. In the Internet of Things, instead of humans, electronic devices communicate over non-secure channels and *physical authentication*, inspired by human biometrics, becomes an important area of research.

A number of works have been presented to implement fingerprints on silicon [5], [6], [7], [8], [9], [10], [11], [12], [13]. The main motivator of silicon fingerprints is the same as human fingerprints: they are unique to each individual and difficult to clone. The challenge is to recognize sources of fingerprints on digital systems, and to quantify their estimated uniqueness and reliability.

We have studied the suitability of MEMS sensors for physical authentication. Such sensors are extensively used to measure physical quantities such as inertia, temperature, altitude, and sound. We utilize the random process variations during manufacturing of the sensor to generate device-unique electronic signatures. In particular, we focus on a MEMS acceleration sensor and use its response to an electrostatic impulse and its uncalibrated measurement outputs as a source of device-unique identifier for physical authentication.

There are two requirements for fingerprint implementations in the Internet of Things. First, for real-time applications, it should be capable of executing at run-time. Second, due to the inherent resource limitations of the Internet of Things, it should be low-cost. SRAM are a popular source for fingerprint generation. However, it has two important disadvantages for Internet of Things applications. First, it requires power-cycling of the SRAM memory that makes it hard for run-time generation, and second, it requires several hundred-bytes of memory locations from a resource which is already scarce in the embedded environment. In contrast, the major advantage of sensor fingerprinting over SRAM-based fingerprints is its memoryless identifier generation. Furthermore, it does not require power-cycling and is continuously available at run-time. Different alternatives for the generation of secret key and motivation of using MEMS are elaborated further in Section 3.2.

1.3 Novelty and Organization

The major contributions of this work are:

- A physical authentication proposal on a MEMS sensor that can be used for low-cost devices.
- A detailed analysis of the physical authentication sources of a MEMS sensor.
- A quantification of the quality of generated digital fingerprints and observations of this method's feasibility.

The rest of the paper is organized as follows: Section 2 presents the security claims of this model and discusses the root of trust. Section 3 briefly discusses previous work, MEMS sensors and the motivaton of using them for physical authentication. Section 4 highlights the key ideas for implementing physical authentication on a MEMS sensor. Section 5 formulates the quantification metrics. Section 6 gives an overview of the target platform, and discusses the design parameters. Section 7 presents the results, and Section 8 concludes the paper.

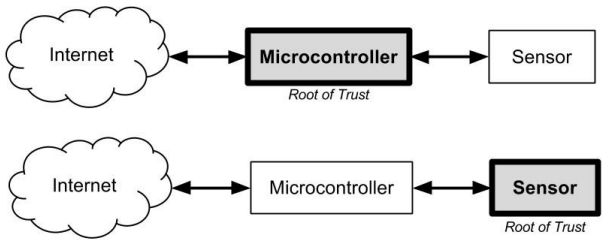

Figure 2. Sources of root of trust

2. SECURITY CLAIMS

The typical application model of an electronic device authentication is as follows. The device manufacturer or the system administrator first enrolls all the unique authentication keys of the authorized devices for the protocol once and stores them in a secure database available to the challenger. During device operation, the challenger will then request the authentication key from the device and compare it with the copy stored in the database. In this scenario, the generation of the authentication keys occurs at run-time, whenever requested, by an enforced mechanism configured by the challenger. We assume the integrity of the execution of code on the microcontroller. The implementation of trusted software execution is a different scope which we do not target in this paper.

The problem that we target is the source of the authentication itself. The traditional means of implementing authentication keys in low-cost devices is to store a factory assigned value in non-volatile memory. Later, the challenger reads this value and checks whether it is listed in the database. There are two drawbacks associated with this method: (i) the authentication key can be tampered with, (ii) the key can be easily cloned to another device by storing a known, valid authentication key to the specific address in memory. The former drawback causes false negative authentications and results in a device misidentification. The latter drawback causes false positive authentications and and enables an adversary to deploy counterfeited devices.

Alternatively, the authentication keys could be produced by utilizing the random process variations that occur during manufacturing. These random process variations provide a biometric-like physical feature for electronic devices which can be used as fingerprints. Because it is difficult to model the process variation, it is also difficult to clone a physical authentication key from one device to another.

2.1 Shifting the Root of Trust

The root of trust is a vital aspect of security in general and more specifically of physical authentication. In the Internet of Things, each sensor will need to be interfaced with a microcontroller (Fig. 2). Traditionally, microcontrollers form the root of trust in a network. Thus, the microcontroller firmware is the source of trust, and the authentication protocol verifies the identity of the microcontroller. However, with MEMS-based fingerprints, the sensor itself becomes a root of trust. The authentication process verifies the identity of the sensor, rather than the microcontroller. MEMS-based fingerprints are therefore one step closer to physical environment of the Internet of Things.

Table 1. Sources of Digital Fingerprints

Resource	Technology scale	Source of Variation	Measured Variation	Overhead of Operation	Reference
SRAM	Nanometer	Electrical	Power-up Values, Write Collisions	Power cycling, True Dual-Port SRAMs	[7],[11],[12]
Microprocessor	Nanometer	Electrical	Execution Results of an Instruction	External High-Precision Clock Generator	[8]
Dedicated Logic	Nanometer	Electrical	Timing of Delay Paths	Dedicated Unit, Reconfigurable Fabric (FPGA)	[5],[6]
MEMS Sensors	Micrometer	Mechanical	Offset Values, Impulse Response	Extra sampling	This paper, [9],[13]

3. MEMS SENSORS

MEMS is a fast growing research area that has been started with micro fabrication of sensors, actuators and electronics. Microsystems have been very important in the field of measurement techniques such as in automotive industry [14]. MEMS devices are composed of micrometer size electronic and mechanical parts that are assembled together. There have been lots of sensors and devices produced by MEMS such as accelerometers, gyroscopes, resonators, microphones and pressure sensors.

3.1 Process Variation on MEMS devices

Manufacturing process of MEMS devices characterizes the properties of their variation [15]. The manufacturing process variation is mainly due to the small fabrication dimensions and high feature complexities. The mechanical features of the devices have variations because of the existence of scatters of material, control voltage, process and geometry parameters. The uncertainty is mostly influenced by parameters such as the cut error, Young's modulus and comb-drive forces which can vary significantly between process runs and even within individual wafer [16]. MEMS engineers use these parameters to evaluate the process variation of MEMS devices. There have been attempts for modeling the process variation in MEMS devices in order to set the system operation in an acceptable range. These methods try to estimate process variations during simulation phase by Monte Carlo [17] or try to reduce its effect during manufacturing phase by the multiphysics approach [18]. Although these probabilistic methods achieve some percentage of accuracy to the MEMS fabrication, there still exists device process variation. In this paper, we utilize these process variations as sources of unique fingerprints which can be used in the authentication protocol.

3.2 Comparing MEMS and CMOS fingerprints

There have been many physical authentication proposals on many platforms. The reader can refer to Maes et al. for a detailed survey of the literature [10]. Table 1 gives the most commonly used sources for generating digital fingerprints, their typical technology nodes, the source of variation, overhead of the operations and the measured variations. The sources that can be utilized are SRAMs, Microprocessors, delays or MEMS sensors.

Generating digital fingerprints using SRAMS is a popular choice [7], [11], [12]. There are two main methods to achieve this goal. The first one is power cycling the SRAM and utilizing power-up values of the SRAM-cells [7], [11]. This method is not practical for run-time authentication key generation. Moreover, Holcomb et al. estimated that to have 128 bit of entropy, 512 bytes have to be allocated within an SRAM [11]. Another method of implementing SRAM-based fingerprint is to utilize the write collision mismatches on true-dual port SRAMs [12]. This method tries to artificially generate a write collision on a dual port SRAM. This method can be implemented without power cycling; however, it can be realized only if the SRAM has true dual-ports

Maiti et al, proposes a novel method using the microprocessor-intrinsic variations for physical authentication [8]. An external high-precision clock generator sweeps the clock input for fingerprint generation. Obviously this also is not very practical for authentication of Things.

Implementation of digital fingerprints using delays of dedicated resources is used since the inception of digital fingerprinting [5], [6]. These methods measure the delays of paths that are intended to be the same by the design, but are different when. Using these methods require carefully designed paths within a dedicated unit (ASIC) or a reconfigurable fabric (FPGA) that is expansive to have on low-cost platforms.

Rosenfeld et al, propose the first MEMS sensor based physical authentication method in [9]. The proposed method uses the measured light level variations of photodiodes. This sensor has an array of on-chip photodiodes and a coating that contains swirls of dark material in a translucent base to provide a medium of non-uniform optical transmittance. The variations between the amounts of light sensed by the photodiodes are used as digital fingerprints. This sensor is specifically built for authentication and has no other use, whereas we propose an authentication method on the general purpose MEMS sensors of the low-cost platforms. Bojinov et al. demonstrates a sensor based authentication for mobile platforms [13]. The proposed method requires measurements collected from six different positions of a mobile device each time for an authentication. This might not be suitable for low-cost devices that are mounted on still platforms. Furthermore, while the initial results of the Bojinov et al looks promising, there is still need for a detailed statistical analysis of the uniqueness and reliability of the MEMS fingerprints.

4. PROPOSED SOLUTION

Physical authentication exploits random process variations during manufacturing of an Integrated Circuit to generate device-unique electronic signatures. A result of these process variations common to MEMS accelerometers is a static offset in the sensor data when 0g acceleration is expected. This 0g offset or bias is an important accelerometer metric because it can have different values for different devices. For example, with an expected offset value of 0g, one device may measure an offset value of 0.1g, while another device measures an offset value of -0.05g.

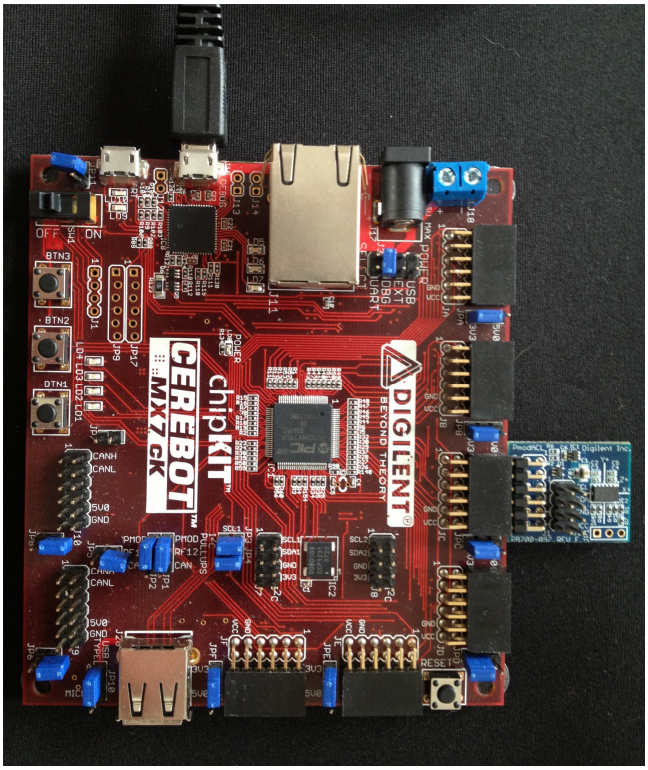

Figure 3. The CEREBOT PIC-32 Board and ADXL345 sensor

Accelerometers are mechanical structures containing elements that are free to move. These moving parts are very sensitive to mechanical stress. Additional stress may be applied to the accelerometer and change the offset value during the assembly phase. This offset can also change due to component soldering, board stress during mounting and application of any compounds on or over the component. Since this offset value is not fixed for each device, we can exploit it as a source of physical authentication.

The authentication process can then be improved by utilizing the offset property in conjunction with the sensor's response to an electrostatic impulse that is exerted upon it. This impulse is commonly present as a self-test feature of MEMS accelerometers. The self-test is defined as the difference between the measured acceleration output of each axis with self-test enabled and the measured acceleration output of the same axis with self-test disabled. When the self-test is enabled, an electrostatic impulse is exerted upon the mechanical sensor, which results in a measured force. This added force causes a shift in the values of the x-, y- and z-axes. Since this shift value is not fixed for each device, it can be exploited as a source of physical authentication; the uniqueness in the shift values can then be combined with that of the offset. Furthermore, this force may be exerted with the device oriented in any position; however, it must remain stationary throughout the duration of the test.

5. BACKGROUND INFORMATION

Two metrics are used for the performance evaluation of physical authentication keys: uniqueness and reliability. Uniqueness (U) is a metric used for estimating how well each device is being authenticated. Therefore the authentication keys of different devices are compared using equation (1).

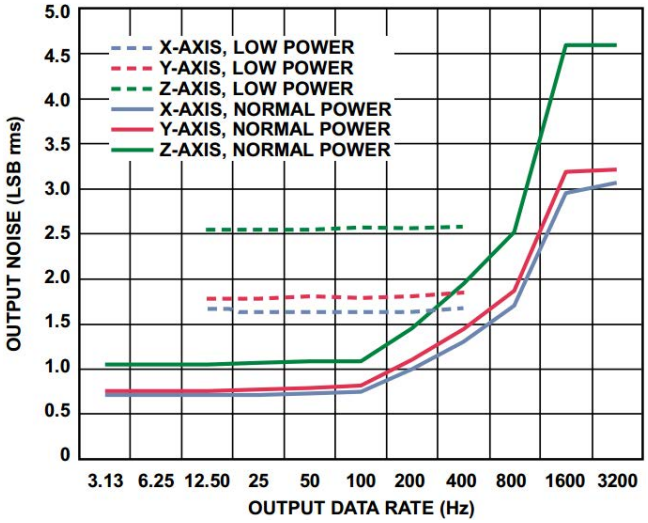

Figure 4. The distribution of ADXL345 x-axis offset values [19]

$$U = \frac{2}{m(m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \frac{HD(R_i R_j)}{n} \times 100\% \quad (1)$$

where R_i and R_j represent n-bit authentication keys of different devices. The total number of devices is m and the metric used for the comparison is Hamming Distance denoted as *HD*. The ideal value of uniqueness is 50%.

Reliability (R) is a metric used for estimating the **A**authentication keys are generated multiple times on the same chip and the generated keys are compared using equation (2).

$$R = 100\% - \frac{1}{L} \sum_{i=1}^{L} \frac{HD(R_i R_{i,L})}{n} \times 100\% \quad (2)$$

where $R_{i,L}$ is the n-bit lth sample of the n-bit response R_i. The total number of samples is L and the metric used for comparison is Hamming Distance denoted as HD. The ideal value of reliability is 100%

6. EXPERIMENTAL SETUP

The ADXL345 is a general purpose, low-power, 3-axis MEMS accelerometer accessible through a serial interface. For this work, the ADXL345 was connected to a development board with a PIC32 microcontroller (Fig. 3). For all measurements, the sensor was stationary, but the position of the board may be arbitrary. Although efforts were made to maximize the stability of the sensor while measuring, it was still susceptible to environmental variables such as vibration, air currents and temperature fluctuations.

When searching for a physical authentication, the ADXL345 data outputs were configured in order to maximize the uniqueness and reliability of the measurements. The device was set to its maximum data output range, which produces a 13-bit value (within a 16-bit word) for each axis. These outputs were then concatenated into a single 48-bit value. . Because the noise in the output values increases with the output data rate (Fig. 4), the measurements were taken at a rate of 100Hz, the minimum rate required by the ADXL345's self-test configuration.

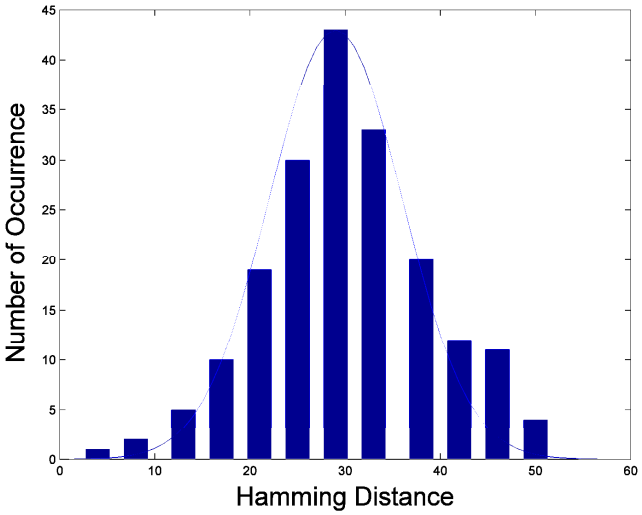

Figure 5. The uniqueness of the offset based physical authentication

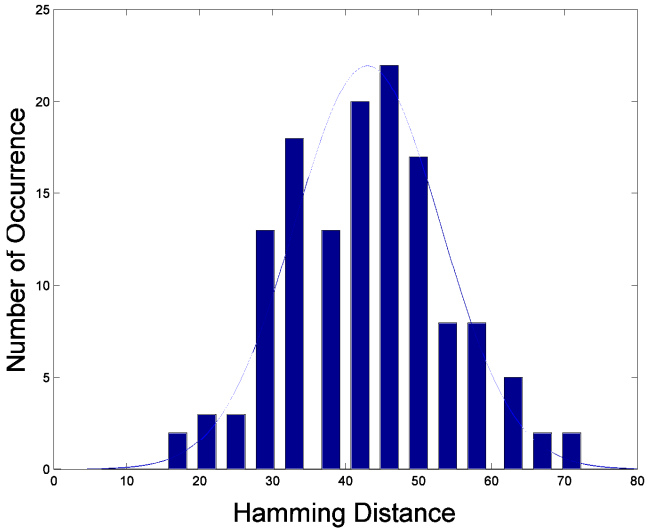

Figure 6. The uniqueness of the self-test based physical authentication

The ADXL345 includes a calibration feature, which serves to minimize its 0g bias by adding a constant value (calculated by the user) to each measurement. Our initial approach simply gathered 1000 samples of the output values from 20 different accelerometers without the use of this calibration, relying only on each device's inherent 0g offset for physical authentication. Our second approach was to exploit the self-test feature of the accelerometer, which exerts an electrostatic force on the mechanical sensor, moving it in the same manner as a natural acceleration. A number of measurements were first taken with self-test disabled and an average value was calculated; this process was then repeated with self-test enabled. The output values were the differences between these two averages, and 100 such outputs were gathered. The self-test of the ADXL345 generates acceleration in a similar direction for all devices. However, there is some variance in the applied self-test force for each device. The acceleration produced by the self-test is additive to the natural acceleration measured by the device (and therefore its inherent offset). The combination of these two unique values improved upon the uniqueness of the offsets alone, and the averaging required by the self-test configuration improved reliability.

7. RESULTS

We have conducted experiments on the ADXL345 to estimate the quality of the physical authentication key. The metrics for this estimation is defined in Section IV as the background information.

7.1 Quality Assessment

We have used a collection of 20 ADXL345 sensors in our physical authentication experiments. All of these sensors can be successfully authenticated using the proposed methods.

Fig. 5 shows the uniqueness results of the physical authentication keys which are generated by the electrostatic force measurements on each sensor. The histogram of the Hamming distances is given in the figure. The mean of these Hamming distances is 30.2 as reported in Table 2.

Fig. 6. shows the uniqueness results of the calibration offset values of different sensors. The histogram of Hamming distances is given. The mean of these Hamming distances is 42.64 as reported in Table 2.

Table 2 gives the uniqueness and the reliability of the authentication keys. We observed that the eight MSBs of the output of the self-test and the calibration outputs in each axis are the same for all sensors and can be dropped to compress the output. The uniqueness of the calibration and self-test is 30.2 and 42.64 respectively. The reliability of the calibration and self-test is 86.23 and 92.17 respectively. We observed that the calibration offset values are less reliable and less unique than the self-test measurements which makes them a less desirable source of physical authentication.

Table 2. Reliability and Uniqueness Results of the Proposed Physical Authentication Methods

Proposed Method	Uniqueness(%)	Reliability(%)
Calibration	30.2	86.23
Self-test	42.64	92.17

7.2 Cost of Operation

The target platforms are often battery-limited and low-power, therefore, it is important to estimate the energy consumption of the proposed digital fingerprint generation. Table 3 gives the typical power and energy consumption for the output sampling of the accelerometer. The target accelerometer has a scalable current consumption which is automatically tuned to reduce the power and energy cost. The accelerometer also has a low power mode that uses a lower current consumption, but this mode is omitted in our experiments, because it introduces more noise to measured outputs [19]. The lowest energy requirement for output data sampling is approximately 0.1 µJ and our experimental setup uses 2.52 uJ to sample one output data.

8. CONCLUSIONS & FUTURE WORK

In this paper, we made an effort towards using accelerometer sensor as a source of physical authentication on low-cost platforms. We have explored the possibility of two sources, namely the self-test measurement and the offset of the uncalibrated sensors to have device-unique values due to process variation. The uncalibrated offset measurements can be applied when the target platform is stationary and self-test measurements can be applied independent of the platform position. The proposed sources can be used as electronic fingerprints for applications that require run-time fingerprint generation without power cycling.

Table 3. Typical Power and Energy Consumption for Various Data Rates

Output Data Rate (Hz)	Idd (µa)	Power (µW)	Energy (µJ)
3200	140	252	0.0788
1600	90	162	**0.1013**
800	140	252	0.315
400	140	252	0.63
200	140	252	1.26
100	140	252	**2.52**
50	90	162	3.24
25	60	108	4.32
12.5	50	90	7.2
6.25	45	81	12.96
3.13	40	72	23.0032
1.56	34	61.2	39.2308
0.78	23	41.4	53.0769
0.39	23	41.4	106.1538
0.2	23	41.4	207

We demonstrated that construction of physical authentication on the ADXL345 accelerometer is viable. The next step could be performing a large scale characterization on a large population of accelerometers for various quality metrics and operating conditions as in RO-PUFs [20]. Our initial results showed that the uniqueness of the raw accelerometer responses are reasonable especially for the self-test measurement. However, these results could be improved by encoding mechanisms. The reliability of the accelerometer responses are arguably insufficient. This issue may be addressed in future works through employing error-correction mechanisms and improvement of the test environment or the accelerometer output sampling mechanisms. Finally, the complete cost of key generation, including the overhead of error correction and encoding, could be quantified.

Our experiments on the ADXL345 accelerometer revealed that, for authentication purposes, the accelerometer related sources are not as unique as SRAM based primitives. However, they can be a low-cost, memoryless alternative.

9. REFERENCES

[1] Bandyopadhyay D., Sen J.: "Internet of Things: Applications and Challenges in Technology and Standardization," Wireless Personal Communications, vol. 58, 2011, pp. 49-69

[2] Philipose M., Smith J. R., Jiang J. R., Mamishev A., Roy S., and Sundara-Rajan K.: "Battery-free Wireless Identification and Sensing", Pervasive Computing, vol. 4, 2005, pp. 37–45

[3] Mitrokotsa, A., Douligeris, C.: "Integrated RFID and Sensor Networks: Architectures and Applications". RFID and Sensor Networks: Architectures, Protocols, Security and Integrations; Zhang, Y., Yang, L.T., Chen, J., Eds.; CRC Press: Boca Raton, FL, USA, 2010, pp. 511–535

[4] Jackson J.: "Ready, aim, record: Army's prototype system uses RFID tags to track weapons use", GCN Government Computer News, http://gcn.com/articles/2008/05/01/ready-aim-record.aspx, 2008

[5] Lee, J.W., Lim, D., Gassend, B., Suh, G.E., Dijk, M.V., Devadas, S.: "A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Application." Proceedings of the Symposium on VLSI Circuits, 2004, pp. 176-159

[6] Gassend, B., Clarke, D., Dijk, M.V., Devadas, S.: "Silicon Physical Random Functions". ACM Conference on Computer and Communications Security, New York, NY, USA (2002), pp. 148-160

[7] Guajardo, J., Kumar, S.S., Schrijen, G.J., Tuyls, P.: "FPGA Intrinsic PUFs and Their Use for IP Protection." Cryptographic Hardware and Embedded Systems Workshop, LNCS, vol. 4727, 2007, pp. 63-80

[8] Maiti A., Schaumont P.: "A Novel Microprocessor-Intrinsic Physical Unclonable Function." International Conference on Field Programmable Logic and Applications (FPL'12), Oslo, Norway, 2012, pp. 380-387

[9] Rosenfeld K., Gavas E., Karri R.: "Sensor Physical Unclonable Functions.", Hardware-Oriented Security and Trust (HOST'10), Anaheim, CA, USA, 2010, pp. 112-117

[10] Maes, R., Verbauwhede, I.: "Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions." Towards Hardware-Intrinsic Security. Springer Berlin Heidelberg, 2010, pp. 3-37

[11] Holcomb, D.E., Burleson, W.P., Fu, K.: "Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers." IEEE Transaction on Computer, vol. 58, 2009, pp. 1198-1210

[12] Guneysu, T.: "Using Data Contention in Dual-ported Memories for Security Applications". Journal of Signal Processing Systems, vol. 67, 2012, pp. 15-29

[13] Bojinov H., Boneh D., Michalevsky Y., Nakibly G.: "Smartphone Fingerprinting: By Their Sensors You Will Recognize Them", Stanford Annual Affiliates Meeting Security Workshop, Stanford, CA, USA, 2013

[14] Eddy, D.S., Sparks D.R.: "Application of MEMS Technology in automotive sensors and Actuators." Proceedings of the IEEE vol. 86, 1998, pp. 1747-1755

[15] Mawardi A., Pitchumani R.: "Design of Microresonators under Uncertainty". Journal of Microelectromechanical Systems, vol. 14, 2005, pp. 63-69

[16] Clark J.V., Garmire D., Last M., Demmel J.: "Practical Techniques for Measuring MEMS Properties." Proceedings of the NSTI Nanotechnology Conference and Trade Show, Boston, MA, USA, 2004, pp. 402-405

[17] Nance R.P., Hash D.B., and Hassan H.A.: "Role of boundary conditions in Monte Carlo simulation of microelectromechanical systems." Journal of Thermophysics and Heat Transfer, vol.12, 1998, pp. 447-449

[18] Bao. M.: "Analysis and Design Principles of MEMS Devices" Elsevier, 2005

[19] Devices, Analog.: "ADXL345 datasheet." USA: Analog Devices, 2010

[20] Maiti A., Casarona J., McHale L., Schaumont P.: "A Large Scale Characterization of RO-PUF," Hardware-Oriented Security and Trust (HOST'10), Anaheim, CA, USA June 2010, pp. 94-99