**Thesis Title Page**

Efficient Implementation of IEEE 802.11i Wi-Fi Security (WPA2-PSK) Standard Using

FPGA

A Thesis Submitted to the Graduate Faculty of

GRAND VALLEY STATE UNIVERSITY

In

Partial Fulfillment of the Requirements

For the Degree of

<name of your degree here>

<your academic unit>

<Month of graduation> <Year of graduation>

# **Acknowledgements**

# **Abstract**

The rationale behind the thesis was to design efficient implementations of cryptography algorithms used for Wi-Fi Security as per IEEE 802.11i Wi-Fi Security (WPA2-PSK) standard. The focus was on software implementation of Password-Based Key Derivation Function 2 (PBKDF2) using Keyed-Hash Message Authentication Code (HMAC)-SHA1, which is used for authentication, and , hardware implementation of AES-256 cipher, which is used for data confidentiality.

In this thesis, PBKDF2 based on HMAC-SHA1 was implemented on software using C programming language, and, AES-256 was implemented on hardware using Verilog HDL. The overall implementation was designed and tested on Nexys4 FPGA board. The performance of the implementation was compared with other existing designs. Latency (us) was used as the performance metric for PBKDF2, whereas, throughput (Gb/s), resource utilization (Number of Slices), efficiency (GB/s per slice) and latency (ns) were used as performance metrics for AES-256. MRF24WG0MA PMOD Wi-Fi module was the 2.4 GHz Wi-Fi module which was interfaced with Nexys4 FPGA board for wireless communication.

When the correct security credentials were entered in the implemented system interfaced to the Wi-Fi module, it was successfully authenticated by a 2.4 GHz wireless router (or mobile hotspot) configured to work in WPA2-PSK security mode. Once this system was authenticated, the implemented AES-256 cipher within the system was used to provide a layer of encryption over the data being communicated in the network.

# **Table of Contents**

[**Acknowledgements** 2](#_Toc528185443)

[**Abstract** 3](#_Toc528185444)

[**Table of Contents** 4](#_Toc528185445)

[**List of Figures** 5](#_Toc528185446)

[**List of Tables** 6](#_Toc528185447)

[**Abbreviations** 7](#_Toc528185448)

[**Chapter 1: Introduction** 8](#_Toc528185449)

[**1.1** **Background** 8](#_Toc528185450)

[**1.2** **Wireless Security Principle** 9](#_Toc528185451)

[**1.3** **WPA2-PSK** 10](#_Toc528185452)

[**1.4** **Project Scope** 12](#_Toc528185453)

[**References** 13](#_Toc528185454)

# **List of Figures**

[**Figure 1: Example of Wi-Fi Network** 9](#_Toc528167596)

[**Figure 2: WPA2-PSK Security** 11](#_Toc528167597)

[**Figure 3: WPA2-PSK Authentication** 11](#_Toc528167598)

[**Figure 4: WPA2-PSK Data Confidentiality** 12](#_Toc528167599)

# **List of Tables**

# **Abbreviations**

# **Chapter 1: Introduction**

## **Background**

As most technologies have continued to transition from traditional wired systems to wireless ones, the number of wireless devices has grown by leaps and bounds over the last decade. Wireless devices have become a part of our day-to-day lives with its presence seen in household, educational and business institutions, to name a few. These devices are inter-connected with one another and share a variety of data, ranging from mundane to very personal and confidential information. Such interconnected devices that share data among themselves form a network. There can be various types of networks based on topology, size, area, organization, etc. One such type of network based on area is called Local Area Network (LAN). Such network is confined within a localized area such as a room, building or a group of buildings. However, it can be inter-connected to other LANs using wired or wireless media. If wireless medium is used to connect such LANs, then the overall network is called Wireless LAN (WLAN) [1].

The communication between the devices within a network is governed by a set of rules called communication protocols. The devices within a network must adhere to such protocols to successfully share and interpret data among other devices connected to the network. To maintain interoperability between the devices manufactured by various vendors, standardized communication protocols are defined for different type of networks. One such protocol for communication between wireless devices over LAN is the IEEE 802.11 protocol and is commonly known as Wi-Fi [2]. An example of Wi-Fi network is shown in Figure 1.



**Figure 1: Example of Wi-Fi Network**

## **Wireless Security Principle**

Security is paramount in any type of network, but it is more so in the case of wireless networks, as they are far more vulnerable to attack in comparison to wired networks. In a wired network, the communicating devices must be physically connected using a cable. Hence, it is easier to verify the identity of the device to which the data is being communicated, as opposed to in wireless networks, where this is not quite easy. Also, unlike in wired networks, where the data is communicated through copper wires or optical fibers, in wireless networks, the wireless devices use RF signals in open air as their communication medium. So, theoretically any transceiver which is within the range of this RF signal and tuned to its frequency can read and/or meddle with the data being communicated [3]. Hence, for a secure communication, it is necessary to identity whether a device trying to connect to the network has proper security credential or not. This process is called authentication [3]. After a wireless device is authenticated to a network, the data being communicated within that network must be made confidential using a secure cryptography algorithm [3].

## **WPA2-PSK**

The current standardized security protocol for Wi-Fi is IEEE 802.11i standard. This is also commonly known as Wi-Fi Protected Access II (WPA2). WPA2 was launched in September 2004 and supports PSK technology and includes an advanced encryption mechanism using the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES) [4]. The PSK technology (in personal networks) is used to verify the identity of the communicating wireless devices. In PSK, the authentication process is performed by the access point (wireless router, mobile hotspot, etc.). With PSK, we can configure the access point (wireless router or hotspot) with a passphrase of 8 to 63 printable ASCII characters [5]. Using a technology called PBKDF2, that passphrase, along with the network SSID, is used to generate unique encryption keys for wireless clients. In WPA2-PSK security, the same set of SSID and PSK is shared between all Wi-Fi end devices and the access point as shown in Figure 2 [6]. The SSID is analogous to Username and PSK is analogous to Passphrase in Figure 2. The wireless devices are authenticated and granted access to the network, if the password to the particular SSID matches [5]. After authentication, AES cipher is used to maintain the confidentiality of the data being communicated within the network.



**Figure 2: WPA2-PSK Security**

In Figure 3, SSID and Passphrase goes through PBKDF2 to derive the 256-bit PMK which is used as the main key for AES cipher. The validity of this key is confirmed using the 4-way handshake process (Figure 2) between the Wi-Fi device and the access point [6]. If the key matches, then, the Wi-Fi device is successfully authenticated by the access point.



**Figure 3: WPA2-PSK Authentication**

After successful authentication, the data between Wi-Fi end devices and the access point is encrypted using AES cipher with the 256-bit PMK as the main key (Figure 4).



**Figure 4: WPA2-PSK Data Confidentiality**

## **Project Scope**

The purpose of this thesis is to optimize the cryptography algorithms used in device authentication and data confidentiality in Wi-Finetworks configured with WPA2-PSK security. To achieve this, the main key derivation part of the authentication process, as well as, the AES cipher algorithm required for data confidentiality will be optimized. The scope of the implementation will encompass the following areas:

* Efficient software implementation of PBKDF2 based on HMAC-SHA1 which is used for device authentication.
* Efficient hardware implementation of AES-256 cipher which is used for data confidentiality.

The performance of these implementations will be compared with other existing designs. Latency (us) will be used as the performance metric for PBKDF2, whereas, throughput (Gb/s), resource utilization (Number of Slices), efficiency (GB/s per slice) and latency (ns) will be used as performance metrics for AES-256.

# **References**

|  |  |
| --- | --- |
| [1] | M. Souppaya and K. Scarfone, *Guidelines for Securing Wireless Local Area Networks (WLANs),* NIST Special Publication 800-153, 2012. |
| [2] | S. Banerji and R. S. Chowdhury, *On IEEE 802.11: Wireless LAN Technology,* International Journal of Mobile Network Communications & Telematics (IJMNCT) , 2013. |
| [3] | J. Edney and W. A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley, 2004. |
| [4] | Wi-Fi Alliance, *Deploying Wi-Fi Protected Access,* 2005. |
| [5] | Juniper Networks, "Understanding PSK Authentication," Juniper Networks, 16 October 2018. [Online]. Available: https://www.juniper.net/documentation/en\_US/junos-space-apps/network-director3.0/topics/concept/wireless-wpa-psk-authentication.html. [Accessed 24 October 2018]. |
| [6] | V. Fadyushin, "Common WLAN Protection Mechanisms and their Flaws," 16 March 2016. [Online]. Available: https://hub.packtpub.com/common-wlan-protection-mechanisms-and-their-flaws/. [Accessed 24 October 2018]. |