ECSE 444 Group 14 Project Proposal

Kai Fan Zheng
260962377
McGill University
Montreal, Canada
kaifan.zheng@mail.mcgill.ca

Niilo Vuokila
260926706
McGill University
Montreal, Canada
niilo.vuokila@mail.mcgill.ca

Noshin Saiyara Chowdhury
260971544
McGill University
Montreal, Canada
noshin.chowdhury2@mail.mcgill.ca

Sarah Ajji
260925797
McGill University
Montreal, Canada
EMAIL

I. Description of Project

Our project will implement public key-encrypted communication between two or more B-L4S5I-IOT01A boards. The project will be completed in a series of modules, and work will be divided accordingly.

A. *RSA Cryptosystem*

The RSA cryptosystem will be used to encrypt and decrypt messages as they are sent and received. The cryptosystem will process output before sending it through the RF communication driver, and upon receiving data from another device. The RSA cryptosystem uses public key and public mod to encode the information and use private key to decode, therefore the third party cannot know the information.

B. *RF Communication Driver*

The RF communication driver handles the inter-device connection data stream. The inter-device communication will be handled by the on-board Wi-Fi chip.

C. *Speaker Output (ringtone)*

The boards will each be connected to a Piezoelectric buzzer which will play back a notification sound whenever a message is received. The ringtone consists of 4 distinct notes, stored in an array of size 22932. Each note is comprised of the fundamental frequency (sine wave) as well as a harmonic. The array is accessed by the DAC through DMA, and the jingle will be played once in normal mode by calling a function. The DAC is driven by a timer at 44.1kHz, resulting in 0.52s of playback per notification sound. The values for playback length were chosen arbitrarily and may be changed in future iterations. The frequencies of each note are not determined yet and will be chosen based on audio preference of the team once a working component is established.

D. *4x4 Membrane Keyboard Functionality*

Each board will be connected to a 4x4 membrane keyboard, which will function as the user's interface for writing a message. The membrane keyboard will be driven by interrupts on the row outputs, and polling on the column outputs. The mapping for each key will be as follows:

1	**2**	**3**	**A**
4	**5**	**6**	**B**
7	**8**	**9**	**C**
*****	**0**	**#**	**D**

Table 1. Membrane keyboard input mapping

This mapping is also subject to change in later iterations. The above is simply the printed layout of many physical implementations of the device.

E. *OLED Screen Output*

The OLED screen will be used to print out the decrypted message for the receiving user, as well as show the user input as it is being typed with the membrane keyboard. The OLED screen component that will be used is SSD1306. This component was chosen due to existing drivers that we will use.

II. Project Milestones & Planned Timeline

A. *Milestones*

For the initial demonstration, we hope to have all the individual components of the system working as intended.

For the final project demonstration, we intend to assemble all the components into a working system.

B. *Timeline*

- Nov 14 - Nov 16: ring tone, keypad, screen drivers ready, manual test each driver.
- Nov 17 - Nov 19: Wi-Fi Rf module driver APIs and crypto System ready, manual test each driver.
- Nov 20 – Nov 22: Integration tests functionalities for each component, manual test combines the components together.
- Nov 23 – Nov 25: Analyzing the feedback from the initial demo, design the user interface, and implement.
- Nov 25 – Nov 28: Put all the components together and test.