Adding Security to 433MHz Wireless Communication

Author: Claudio Ferreira Dias

Date: December 6, 2016

Introduction

The industrial, scientific and medical (ISM) radio bands are an unlicensed part of radio frequency spectrum used for general data communications. Among the devices operating in these 433.92/868.35 MHz bands are Wireless doorbells, garage door openers, Wi-Fi, Bluetooth. Wireless interface modules for ISM band are low cost and widely available. But despite their broad use, most do not incorporate security protection. This is becoming increasingly important with the growing use of IOT and home automation. In this application note, we present how to transmit signals securely by adding pseudo random coding when using low-cost transmitter and receiver modules.

The GreenPAK SLG46120V IC is used to generate data coding while GreenPAK SLG46722V performs decoding. Typical issues such as noise with the regular wireless systems will be pointed out.

Transmitter and Receiver Modules

We chose to use modules for wireless transmission because of their wide availability and low cost. Table 1 shows features commonly found on such modules.

	Transmitter	Receiver
Frequency	433 MHz	433 MHz
Power	25 mW	-
Working Voltage	5 – 12 V	5 VDC
Working Current	40 mA (MAX)	5.5 mA (MAX)
Modulation	FSK/ASK/OOK	FSK/ASK/OOK
Speed	Less than 10 kbps	Less than 10 kbps
Bandwidth	2 MHz	2 MHz
Sensitivity	-	-100 dBm @ 50 Ohm
Coverage	200 meters	200 meters

Table 1. Most common modules characteristics

Although modules are available in different designs, they share default pinout. Figure 1 shows two modules used in this application note: a transmitter on the left side and a receiver on the right side.

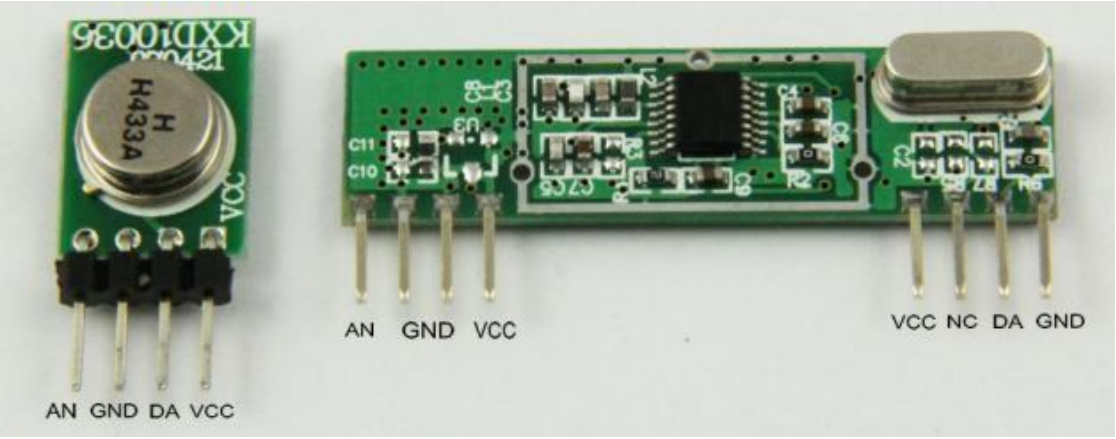

Figure 1. Wireless modules

The pins of the modules are AN, GND, DA, VCC, and NC. The AN pin is used to connect the antenna. It is possible to use the module without an antenna for short distances, but an appropriate antenna will significantly increase the coverage area effectiveness. The antenna can be a simple 23 cm piece of wire. Furthermore, the transmission power depends on the working voltage applied to the transmitter ranging from 5 – 12 VDC. The VCC and GND pins are used to power the circuits and voltage limits must be verified from Table 1. The designer must be careful because the working voltage is different between the transmitter and receiver. If you are not sure, then you can use 5 Volts for both designs. The DA pin is used to transmit or receive data which is transferred serially at the maximum rate of 9200 bps. The NC pin stands for non-connected, and it must be isolated.

Pseudo Random Noise Coding

Pseudo random noise is a signal similar to noise which satisfies one or more of the standard tests for statistical randomness. At first sight, the sequence may look undefined, but it consists of a deterministic stream of data that will repeat itself after a period. The properties of pseudo-random noise play a fundamental role in cryptographic devices ensuring secure communication. A cryptographic device can produce a key signal that has a very extended period and can reach even millions of digits.

The main reason for the better security resides on a feature of pseudo random noise which has a period sequence with little correlation to any other sequence. Furthermore, by taking two subsets of the period, it will also result in a weak correlation. Besides, unlike random noise, it is easy to generate the same sequence at both transmitter and the receiver. The receiver can locally generate the same sequence as the one produced by the transmitter and become synchronized using correlation properties.

In this project, we rely on the features of a maximum length sequence (MLS) which is a type of pseudorandom binary sequence. A periodic bit sequence of an MLS has sequence length N=2^n-1, where n is the degree of a polynomial. The sequence can be generated using maximal linear feedback shift registers (LFSR) digital circuit as highlighted in Figure 2. The degree of a polynomial n indicates the number of required registers.

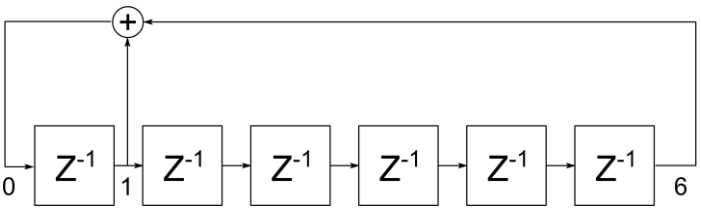

Figure 2. LFSR for generating a 63 bits sequence

Registers are in a stream where the output of the first feed the input of the next. Some outputs connect to the modulus-2 sum operator, and the result is feedback to the first register in the line. The polynomial $x^6 + x + 1$ represents an LFSR structure according to the Galois Field (finite field arithmetic) of two elements, GF(2). The illustrated structure in Figure 2 has degree n=6 and length of $N = 2^6 - 1 = 63$ bits. The designer must pick one of the options listed in Table 2, because not all polynomials can produce full $N = 2^n - 1$ bits sequence.

Solution Architecture using GreenPAK3

The SLG46120V IC was chosen to implement the functions of the secure transmitter.

Degree(m)	Length of the m-sequence(N)	Polynomials
3	7	$x^3 + x + 1$
4	15	$x^4 + x + 1$
5	31	$x^5 + x^2 + 1$
6	63	$x^6 + x + 1$
7	127	$x^7 + x + 1$
8	255	$x^8 + x^7 + x^2 + x + 1$
9	511	$x^9 + x^4 + 1$
10	1023	$x^{10} + x^3 + 1$

Table 2. Maximum Length Sequence polynomials

There are five combinatorial look up tables (LUTs), eight clocked digital flip-flops (DFFs), one eight-stage pipe delay, and an RC oscillator with two selectable frequencies. All these components fulfill the requirements to implement the design for a transmitter. Figure 3(a) shows the top level schematic which reveals how GreenPAK SLG46120V IC and the wireless module are connected together.

Since the receiver is more complex, the SLG46722V part was chosen to realize such functions. Figure 3(b) shows the top level schematic for GreenPAK SLG46120V IC and wireless module connections. The available resources are fifteen combinatorial look up tables (LUTs), seven clocked digital flip-flops (DFFs), one eight-stage pipe delay, two deglitch filters, and an RC oscillator with two selectable frequencies. All these components fulfill the requirements to implement the design for receiver.

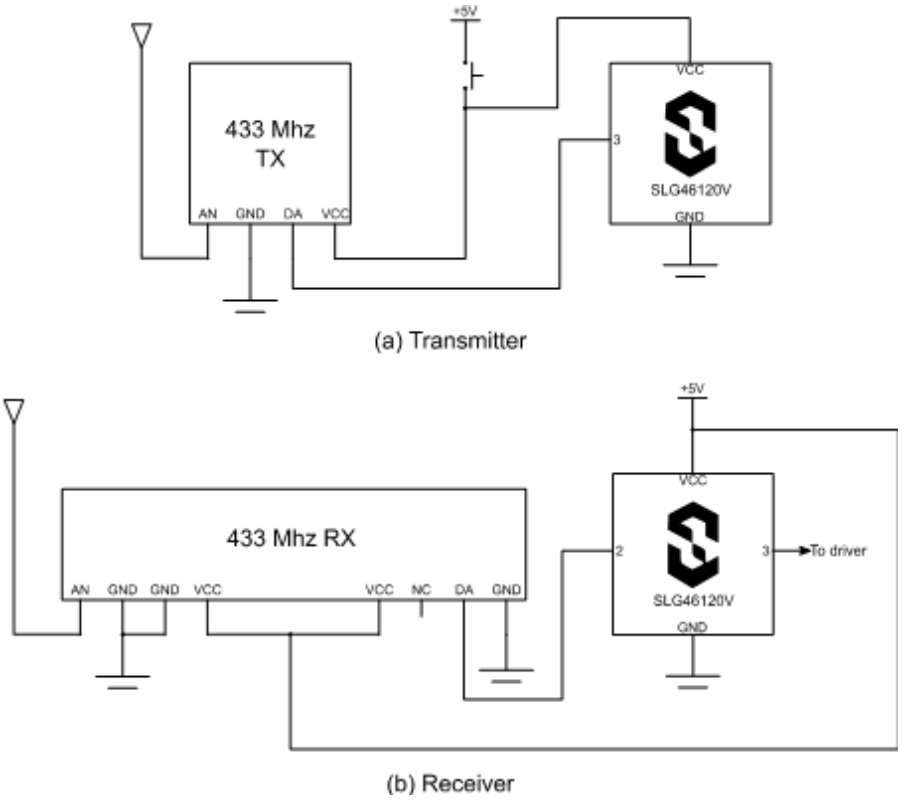

Figure 3.TX/RX top level schematics

The LFSR design presented in Figure 2 is now carried out in the GreenPAK development environment as can be observed in the diagram highlighted in Figure 4. This design will play the role of the transmitter to generate a sequence of 63 bits to the wireless modules. It consists of a stream of six DFF's and one XOR logic operator acting as module-2 sum operator. The module-2 sum operator feedbacks the input of the delay structure and receives signals from the first and last register outputs representing the polynomial discussed in the previews section. Another important detail about the LFSR is that some registers of the stream must have initial state set. If all registers of the delay structure have initial state zero, then the modulo-2 operator has no bits to feedback, and the problem can be solved just setting the first to initial state one. The sequence of 63 bits is taken from the end of the registers stream and fed to the pin 3 which is a digital output. The designer must be aware of the connections and configurations of the oscillator. The power down pin of the oscillator must connect to the ground GND. Notice also that some DFF's registers have reset input pins which must connect to VDD.

According to the Table 1, the average speed of the wireless receiver is less than 10 kbps. It is not possible to achieve exactly the rate of 10 kbps with the current combination of dividers present in the oscillator settings. Thus, the transmission rate closest to the maximum limit of the wireless module is 6250 bps in which the oscillator operates with 25 kHz clock and pre-divider set as 4. It is also possible to use the second 2 MHz clock and achieve a faster speed using a pre-divider of 4 and the 'OUT0' second divider configured as 64 which results in 7812.5 bps. Figure 5 shows a clock configuration table for two different rates.

The receiver side has similar design to the one presented in the Figure 4, and Figure 6 shows the actual implementation. The receiver design will process the sequence of 63 bits received by the wireless module. The main part of this concept also relies on the structure of six DFF's and one XOR logic operator acting as module-2 sum operator. The difference is that this time the module-2 sum operator will not feedback the input of the stream, but still receive signals from the first and last register outputs.

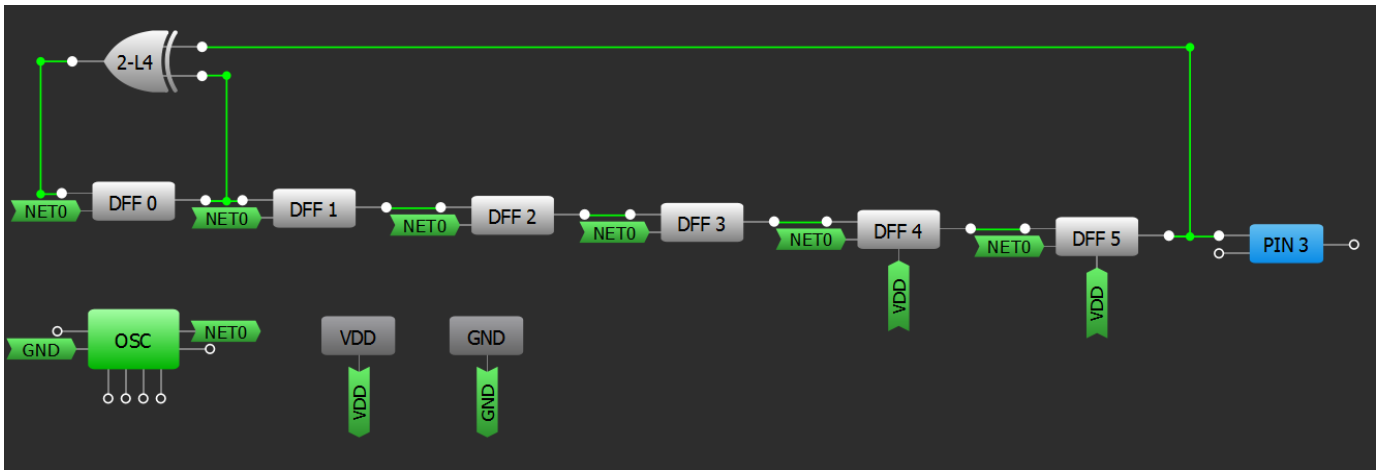

Figure 4. LFSR implementation using GreenPAK Designer

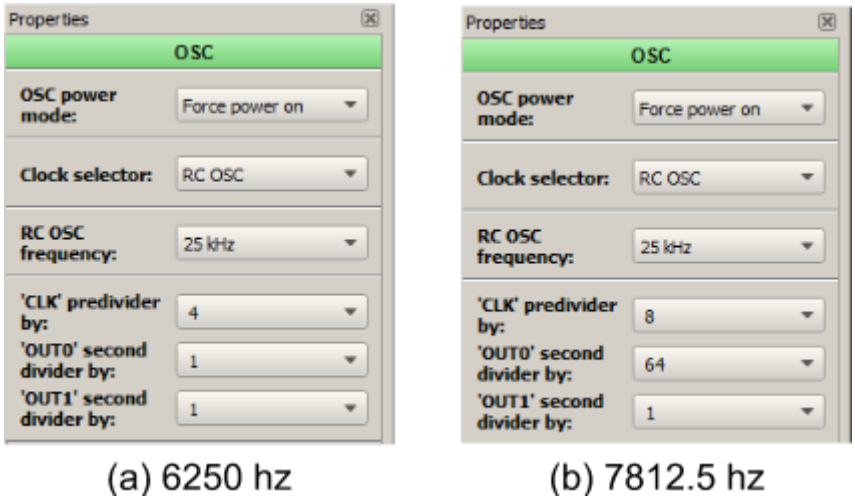

Figure 5. Two clock rate configurations

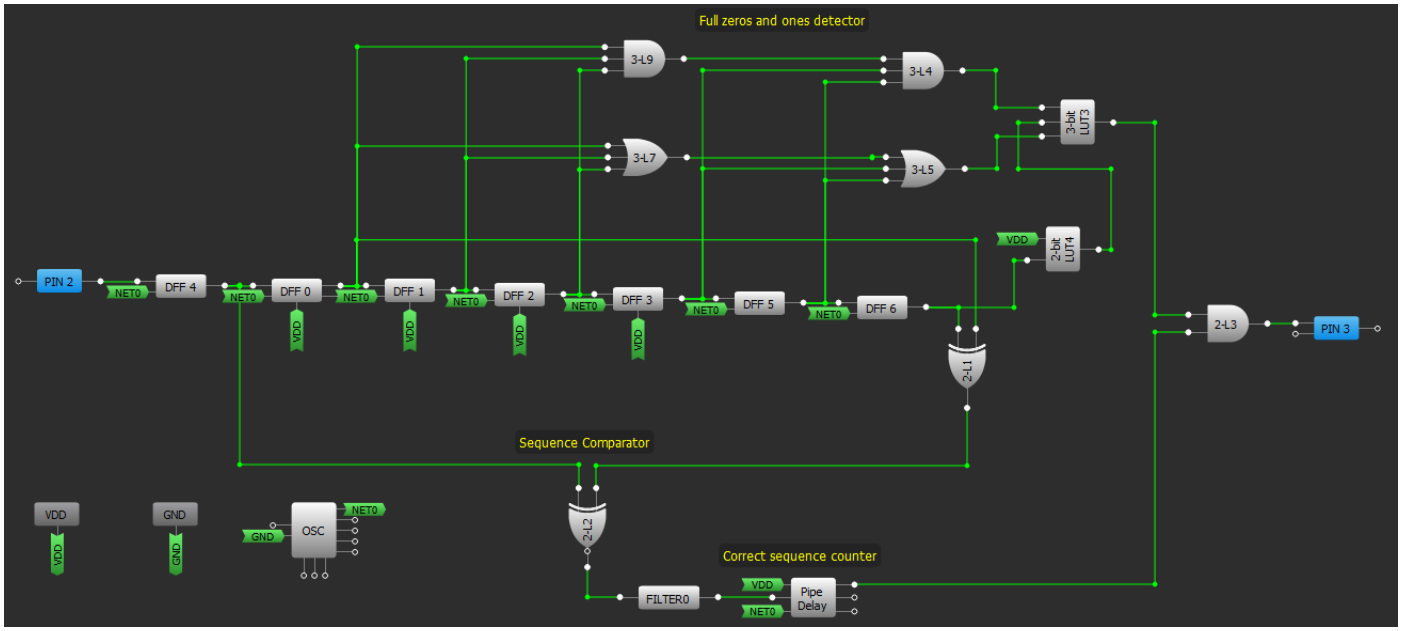

Figure 6. LFSR-like implementation in the receiver

The sequence of 63 bits comes from pin 2 which connects to the wireless module. The module-2 operator of the receiver compares the locally generated bits to the incoming stream from the pin 2. If all bits match, then the received sequence is correlated with the local sequence generator polynomial.

An inverted XOR operator compares the input and locally generated bits denoted as 'sequence comparator.' The output feeds the reset port of a pipe delay which is the structure denoted as 'Correct sequence counter.' The output of pipe delay sets its output OUT0 to one after a determined amount of correct bits.

Every wrong bit match resets the pipe delay. The OUT0 port of the pipe delay connects to one terminal of the NAND 2-L3 port. The other 2-L3 NAND terminal receives signals from a chain of LUTs denominated 'Full zeros and ones detector' which prevents the output going high when there is an incoming sequence of zeros and ones. The sequence of the transmitter and the receiver are the same when all 63 bits of the sequence matches. The pipe delay has eight delay registers connected in a row which can be simultaneously reset. Notice that using just a pipeline delay will only count 16 correct bits and set to one the output OUT0. One trick to solve this issue is to use a counter configured to increment up to 4 and connect it to the clock of the pipe delay. Notice that by using this approach some of the bits in the 'Sequence comparator' will be ignored and naughty bits of the evaluated sequence will pass through without evaluation. Another solution, which can count less than 63 bits, is to extend the pipe delay by using more DFF registers. If the designer is planning to use a smaller pseudo-noise sequence, then there are four extra DFF's in the SLG46120V IC with reset port. The new DFF's can connect to the output OUT0 of the pipe delay and the reset ports attached to the 'Sequence comparator' achieving the counting limit of 20 bits.

Considering that the transmission speed covered earlier, it is possible to calculate the amount of time required to transmit all 63 bits. The formula to calculate the transmission time is $t_{pn} = N_{pn}/R$, where N_{pn} is the total amount of transmitted bits, R is the transmission rate. For $N_{pn} = 63\ bits$ and $R = 6250\ bps$, the transmission time is $t_{pn} = 10\ ms$.

Wireless module noise considerations

Noise issues are a common problem present in many 433 MHz wireless modules. When there is no signal on transmission, the digital output of the receiver module produces a random set of one and zero bits. Figure 7 illustrates a signal plot showing the input noise behavior. The 'noise' section shows when there is no signal on transmission, 'wake up burst' usually happens when the receiver RF front end adjusts the gain control, and the 'data' section shows the actual transferring information. When using microcontrollers, the firmware coding must be very efficient to deal with the random burst of signals in the input port. Usually, interruptions are used to trigger a start transmission event, and random input bits keep triggering the interruption structure constantly. Depending on the code implementation, this might yield malfunctioning, and the microcontroller will fail to receive the transmitted signal.

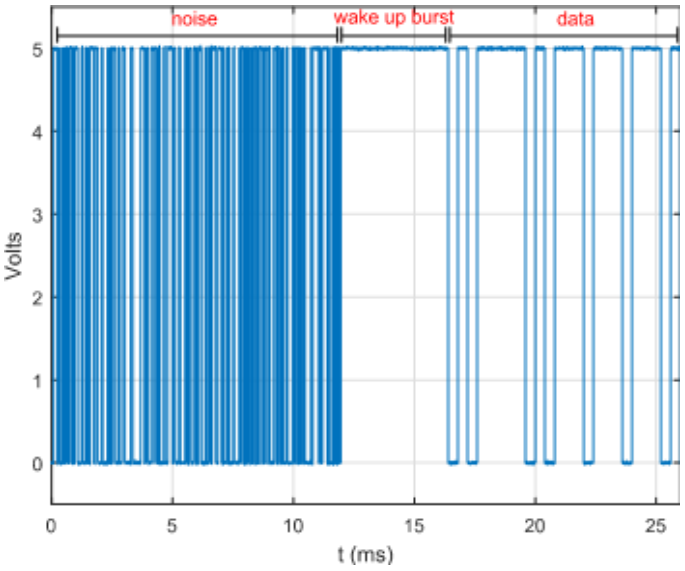

Figure 7. Start transmission event

The advantage of using GreenPAK IC resides in the dedicated function for receiving the data information. Even if a burst of random excitation comes through the input pin 2, all bits will be evaluated by the same logic circuit without any interruption. Thus, the decoding is more efficient, and it is software bug proof.

Design Test

The first test is performed to show how the circuit behaves with direct signaling(no wireless). In direct signaling, pin 3 of the transmitter design (shown in Figure 4) is directly connected to the pin 2 of the receiver design (shown in Figure 6). Both designs were tested with a logic analyzer. Figure 8 shows the output signals taken from specific points in the receiver design.

The 'Direct transmitted signal' plot derives signals from pin 2. The 'Sequence comparator' plot shows results of the XOR operator output which compare the input signal with a locally generated sequence. The 'Pipe delay' plot highlights the moment when there are eight successful counts and the output pin 3 is set High. The 'Oscillator OUT0' plot aids to check if the clocked events are working properly. Notice that the 'Pipe delay' sets one within eight clock counts after the last reset pulse from the 'Sequence comparator.'

The second test is performed to show how the circuit behaves when using the wireless modules. The transmitter design connects to the DA pin of the module to the left in Figure 1. Then, pin 2 of the receiver design connects to the DA pin of the module to the right in Figure 1.

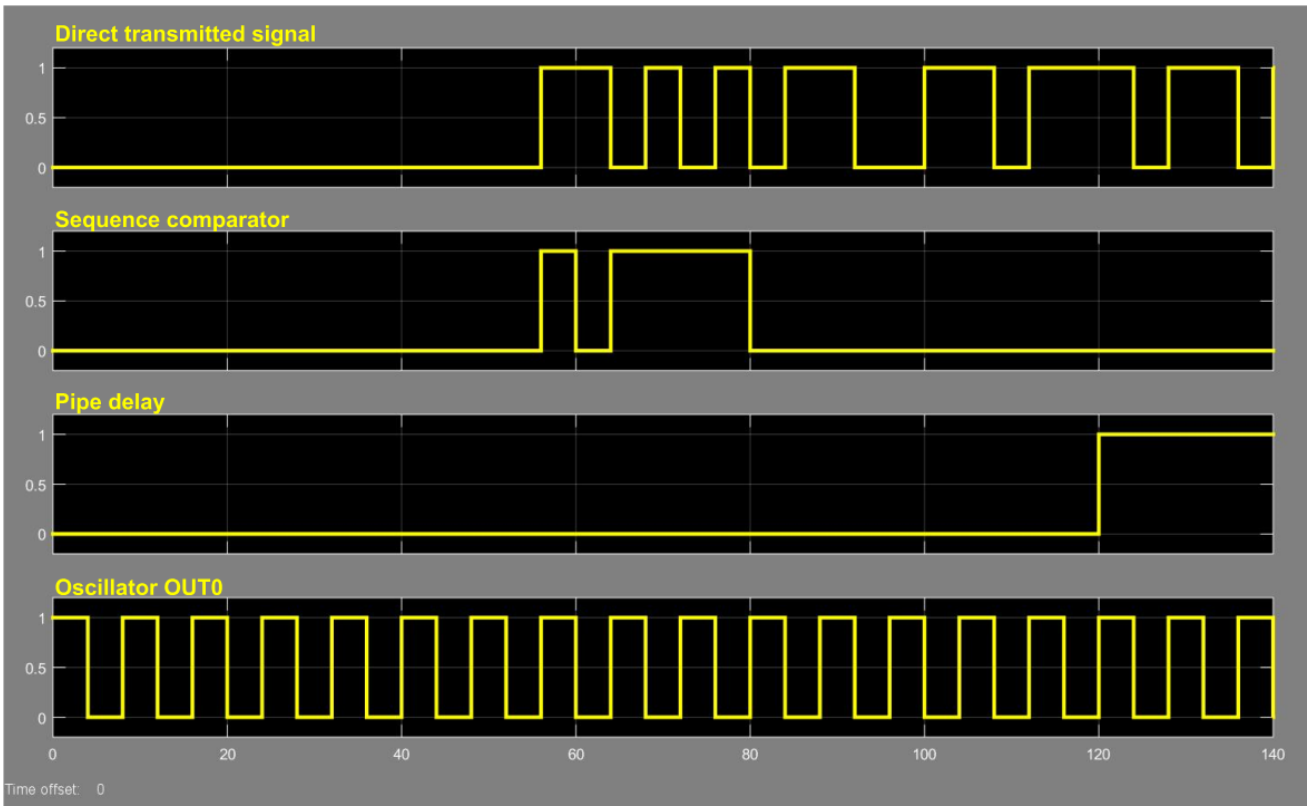

Figure 8. Logic analyzer outputs for TX/RX directly connected

Figure 9 shows the output signals taken from specific points in the receiver design. The 'Wireless module receiver' plot derives signals from pin 2. The 'Sequence comparator' plot shows results of the XOR operator output which compares the input signal with a locally generated sequence. It is evident that 'Sequence comparator' is now producing more resetting signals. The 'Pipe delay' plot, which is configured with only eight registers for the sake of illustration purposes, highlights the moment when there are eight successful counts and the output pin 3 is set High. Again, the 'Pipe delay' switches from zero to one within eight clock counts after the last reset pulse from the 'Sequence comparator.' An interesting observation in Figure 9 is the existence of shorter pulses in the sequence comparator. The reason for the shorter pulses is due to the rate of the logic analyzer operating at a sample rate of 25 kHz.

Observe that shorter pulses are also similar to the behavior seen in Figure 7 which happens only on the first eight clock pulses. Those are the input noise pulses coming from radio static.

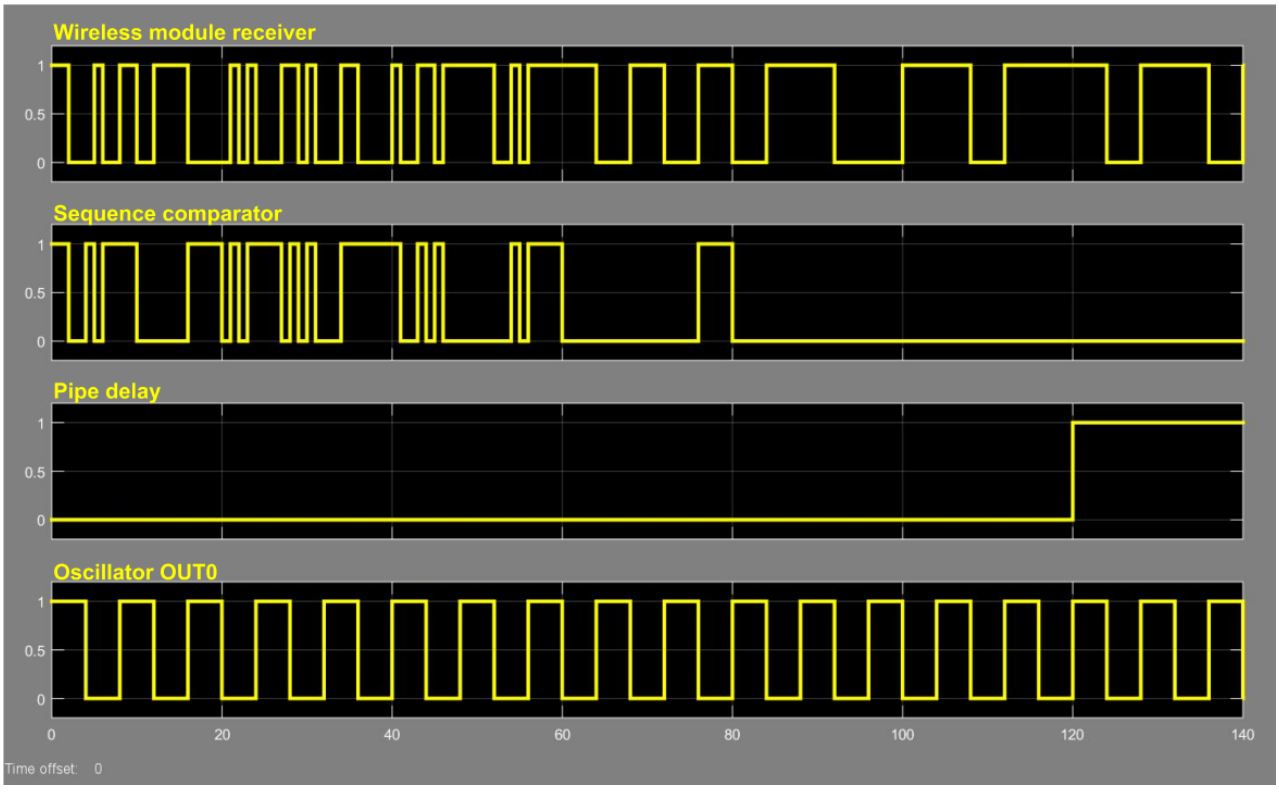

Figure 9. Logic analyzer outputs for TX/RX connected by wireless modules

Conclusion

We proposed adding pseudo random coding for improving data communication security of wireless modules. The design worked according to what was expected as verified by the logic analyzer results.

The GreenPAK SLG46120V and SLG46722V provided the circuit resources for designing this application. The timing control is easy to configure, and there are enough circuit resources available to produce a random sequence of 63 bits.

The designer has flexibility to choose different unique codes, which can be generated by using a new sequence generator polynomial. This approach offers far more security than standard 8 bit wireless garage door controls.

IMPORTANT NOTICE AND DISCLAIMER

RENESAS ELECTRONICS CORPORATION AND ITS SUBSIDIARIES (“RENESAS”) PROVIDES TECHNICAL SPECIFICATIONS AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for developers who are designing with Renesas products. You are solely responsible for (1) selecting the appropriate products for your application, (2) designing, validating, and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. Renesas grants you permission to use these resources only to develop an application that uses Renesas products. Other reproduction or use of these resources is strictly prohibited. No license is granted to any other Renesas intellectual property or to any third-party intellectual property. Renesas disclaims responsibility for, and you will fully indemnify Renesas and its representatives against, any claims, damages, costs, losses, or liabilities arising from your use of these resources. Renesas' products are provided only subject to Renesas' Terms and Conditions of Sale or other applicable terms agreed to in writing. No use of any Renesas resources expands or otherwise alters any applicable warranties or warranty disclaimers for these products.

(Disclaimer Rev.1.01)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Contact Information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit www.renesas.com/contact-us/.

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.