Introduction

Houses have physical access systems to keep intruders and home invaders out. These systems can take on many forms: radio frequency identification (RFID) systems, old-school lock and key, or even a receptionist to fend off social engineering tactics in a residential building. Needless to say, residents must be confident in the protection offered by these barriers to feel safe inside their homes.

In many homes, aside from the main door, the garage door serves as an initial barrier. However, an intruder might see the garage door as a discreet option for breaking into a house. Once past that, they can figure out several ways to go break in further, such as accessing an elevator in the building or even abusing emergency boxes to disable the locks of doors inside the house. But first they must enter the garage without attracting suspicion. One way they can do this is by using a remote to open garage doors.

Well-known experiments on automatic garage door security have been done before. However, an opportunity to revisit this attack scenario presented itself in the form of a broken garage door remote that needed to be replaced — in this case, that of the researcher. This circumstance gave us the idea of testing two attack scenarios that bypass the rolling code protection implemented by most automatic garage door mechanisms.

We began the test by capturing and analyzing the signals sent by each remote button push using Software-Defined Radio (SDR). During the analysis, we show a hidden feature shared by several brands of remotes that is used in many installations. This hidden feature is essential in our first attack scenario where we see how it can be used to register a new remote to the receiver and get permanent access to the garage. We also introduce the rolling code mechanism used by the remotes and the known ways to bypass that protection. The last part of this article introduces PandwaRF, a tool that shows that it is possible to conduct such attacks in a very discreet and stealthy manner.

The Remotes

The remotes used for this article are S449-QZ2 remotes, which cost approximately €10 each (around US$12 as of this writing), and receivers that support these remotes, like the Cardin RMQ449200, which cost approximately €50 (around US$58 as of this writing), as seen in Figure 1. We chose Cardin because it is one of many systems that we use in one scenario, which we introduce in the next section.
The two buttons serve as the authenticated remote, and the four-button remote serves as the remote we will introduce to the receiver later on. To begin, we need to record the first remote into the receiver's electrically erasable programmable read-only memory (EEPROM) using its manual “MEM” button and follow the step described in the provided manual.

For an attacker, this will be a straightforward step if the receiver is exposed outside without any physical security mechanism. Indeed, in such a scenario, it would be easy for an intruder to record his own remote and get in. But thankfully, receivers are typically kept in a metal box inside the locked garage, so potential intruders would need to first get inside by slipping in without being seen while a vehicle passes through — or they could find some other way of getting to the receiver without raising suspicion. It is only after doing so that they can eventually record a new remote to get permanent access or find a stealthy way of getting out of the premise without having to damage the mechanical opening.
In this article, we study the signal sent by the remote and learn its possible uses. But first, let us introduce a feature that is present in many systems, called the DOR procedure.

The DOR Procedure
The meaning behind the acronym “DOR,” which is used to name this feature, is not stated explicitly in the manual. However, after reaching out to the creator of PandwaRF, Djamil Elaidi, for our research, we now know that this acronym refers to “direct on receiver.” The Cardin RMQ449200 manual (Figure 3) reveals how this is a procedure on how to remotely record a remote using a hidden button. This hidden button is seen more clearly after disassembling the remote, as shown in Figure 4.
Figure 3. Instructions for the DOR procedure with a hidden button

Figure 4. Image of the disassembled remote and the DOR’s "hidden" button (in the red box)

The DOR procedure described in the manual is a fast and easy way to record a new remote with the help of an authentic one. If the DOR button is activated by a button push, the receiver should play a sound to notify users of this state. It is important to reiterate that the DOR functionality is relatively common and can be found in devices made by other manufacturers other than Cardin.

**Making Captures**

Now that we have introduced the remotes and the DOR feature, we can move on to capturing the signal. To do so, we first identify the frequency range used by the devices. This information can be collected through a little investigating: by looking at the Radio Frequency (RF) chip used by the remote, which appears to be a TDA5150 (Figure 5) that is used for 300 to 928 MHz bands. Looking at the printed circuit board (PCB) itself narrows the range further, as it shows either 433 MHz or 868 MHz (Figure 6).
Figure 5. The PCB of the remote with a Microchip microcontroller (in the red box) and a TDA5150 transceiver (in the blue box)

Figure 6. The back of the PCB with information about the possible bands
These central frequencies correspond to European industrial, scientific, and medical (ISM) bands, which are interesting to monitor, particularly in internet of things (IoT) devices.

Aside from these two indicators, sometimes the vendor can also directly just give the exact frequency of their product, as was the case for our test remote.

![Figure 7. Our test remote's ID and the precise frequency it uses](image)

With this information, we can now use a custom Software-Defined Radio (SDR) frequency analyzer with a simple flowgraph that will display a fast Fourier transform (FFT). There, we observed two spikes relative to a 2-FSK/BFSK by looking at the space and mark level, as seen in Figure 8.

![Figure 8. Waterfall showing the mark and the space of the 2-FSK transmission](image)
This signal is also a deviation of 20 kHz, a piece of essential information that one needs to keep in mind when demodulating this signal. We can then record this signal using a complex file sink since we will use this for further analysis without having to push any button.

Note that we can try using a lower sampling rate to better match the bandwidth of our signal. However, SDR is limited to a minimum and a maximum sampling rate depending on the analog-to-digital converter (ADC) chip and the baseband (BB) antialiasing filters (if supported) to perform decimation.

For our case, using a Universal Software Radio Peripheral (USRP), we can begin with a sampling rate of 1 MSps, which works fine even with most SDR devices, and then decimate within a software filter. For optimization, we can try lowering the sampling rate to see if we will still get the same results.

As a result of using a filter and optionally decimating it by 10 to spare us the effort of extra computing, the GNU radio companion (GRC) flowgraph to capture our signal will therefore look as pictured in Figure 9.

![Figure 9. GRC flowgraph to capture button presses in a complex file with decimation](image)

**Demodulating the Signal**

Before demodulating the signal, let us look at the FFT to see how we can clean the signal with a squelch to remove some noise.

![Figure 10. FFT of the captured signal](image)
It should be noted that we can refine the low-pass IQ filter further to only let the desired band pass. We can then proceed to demodulating this signal with an FM or a quadrature demodulation block by defining a sensibility relative to the deviation as seen in the following equation:

\[ Gain = \frac{1 \times 10^6}{2 \times \pi \times \left( \frac{20kHz}{2} \right)} \]

Figure 11. The flowgraph to demodulate the captured signal

The result of the demodulation gives us some interesting data.

Figure 12. The demodulated signal

Now that we have demodulated the signal, we can now move on to decoding this little signal to get relevant data.

**Extracting the Data**

Before decoding the signal, we will have to find the samples per symbol rate. This is because both symbols, 0s and 1s, get repeated several times among the samples so that the receiver can synchronize with these symbols. To simulate that action, we can record the signal to "wav" and look at the number of
samples it takes to get a "0" or a "1" through Audacity or another powerful tool like Inspectrum, which we used for this test.

![Figure 13. Looking at samples per symbol rate in Inspectrum](image)

We can clearly see that our symbol period is around 410 μs (most likely 400 μs), so the samples per symbol rate should be 40. We can then use this value in the Symbol Sync block, replacing the Clock Recovery Mueller and Mueller (M&M) block in the new versions of GNU Radio. Then we use a threshold value to extract clear 0 and 1 symbols, pack all bits to bytes, and record them into a text file. This flow can be seen in Figure 14. The data recorded into our file sink at /tmp/decoded_data can be seen in Figure 15.

![Figure 14. The flowgraph to extract the relevant data into a binary file](image)
Note that the squelch and threshold should also be adjusted to the captured signal gain and spike drops. Optionally, an automatic gain control (AGC), which helps control the received signal strength, can be put before the synchronization if the signal is weak or the gain is unstable. We can also choose to leverage the weak signal manually. Afterward, it is advised to convert bytes into binary and apply a good alignment based on the preamble.

We can then try all commands and compare each button push to figure out the different fields in the packets in blind, but doing this work manually can be time-consuming. Rather, there exist tools that would allow the reversal of the different fields and compare pushes more efficiently.

**Decoding the Data**

To decode the data, we use the Universal Radio Hacker (URH) tool, which would allow us to record, demodulate, and compare different pushes. But first, let us analyze and guess the potential fields using URH.
We can see that many instances of "100" and "110" appear in the packet after the preamble, leading us to use the popular Pulse Width Modulation (PWM) encoding instead of Manchester encoding. Therefore, using URH, we can create a decoder that will substitute "110" with "0" and "100" with "1." The result can be seen in Figure 18.

![Figure 17. Making a decoder in URH](image1)

![Figure 18. The PWM-decoded button press](image2)

We have been able to identify the preamble with only one sample. Therefore, we will have to keep going by pushing the same button again to observe the presence of the rolling code and try to guess other fields using an additional remote.
Note that we do this for the two buttons that we will label as A and B and the hidden button related to the DOR feature mentioned earlier.

After recording several different pushes, we can identify fields like the command field, the fixed part, and an encrypted part, which indicates that the remote is protected by a rolling/hopping code mechanism.

Looking again at the microcontroller chip, we can see an "M" logo, indicating that this chip is probably made by Microchip. While it is hard to find the reference and get the datasheet of this chip, we can refer to the KeeLoq algorithm, which Microchip natively uses for a rolling/hopping code.

**Analysis of the DOR Command**

Comparing the DOR command to the buttons we have labeled as A, B, C, and D of a remote — the latter two are only seen in the four-button test remote — shows no difference in the structure. We have the fixed part, an encrypted ID, and another encrypted part with the hopping/rolling code. But there is something strange with the DOR command: We can replay it.

If we try to send this same command multiple times, we can see that we can replay it without a problem for the receiver, which will accept it only until the rolling code is exhausted by any of the A, B, C, or D buttons.

This process is what allows for a plausible attack plan, as illustrated in Figure 20.
As described in Figure 20, we need to sniff the DOR command, then block the first button press by jamming it while also recording it. The procedure will fail as a result, which should allow us to directly replay the DOR button of the authenticated remote, play its button A, and record our remote by sending its button A, B, C, and D signal.

We can also skip the first pushes and jam the remote maintainer to register and record our remote instead. But this technique would require us to capture both a valid button A and DOR key presses which, in a real scenario, would be rare unless the would-be intruder has physical access to the remote of a resident (even for just few seconds), or if they had the chance to meet the maintenance personnel tasked with programming a new remote.

**The Rolling Code**

Now we proceed to testing the second scenario. Let us see if and how we can go against the rolling code in use. Much of this might already be familiar to those in the industry, but it can perhaps serve as an introduction to others who are studying similar threat scenarios.
Microchip's KeeLoq

As mentioned earlier, Microchip uses its own proprietary KeeLoq algorithm to protect the packet from being replayed and decoded. There are two types of KeeLoq mechanisms: a hopping code, which we use in our case, and an Identify Friend or Foe (IFF), which relies on a challenge-response.

In our context, a rolling/hopping code is generated in the format illustrated in Figure 21.

![Figure 21. Format of KeeLoq encoded messages](image)

To encode the messages, the transmitter has several elements to fetch from its on-chip EEPROM, some of which are the following:

- The 64-bit encryption key
- Synchronization counter
- Serial number

![Figure 22. How KeeLoq encodes the messages](image)

For each keystroke, a message is generated with fresh, new encrypted data. Packets also cannot be replayed, as the receiver (in our case) will look for the keystroke with a sync counter +1.

Microchip used to propose to the vendors an algorithm depending on the serial number and a 64-bit manufacturer key to generate the crypt key. Using the crypt key, it is possible to encrypt or decrypt the second part of the message.

Moreover, the source of KeeLoq has been published and released to the public in the past. As a result, although it is now considered confidential and subject to a license, it is still possible to find the leaked source code of the algorithm.
Attacks on KeeLoq
Like many rolling/hopping code mechanisms, KeeLoq does not have any nonce or timestamp preventing an attacker from recording two successive pushes by jamming them, replaying the first one, then using the second one to discreetly open a door. This attack was demonstrated by Andrew Macpherson and Mike Davis in a video. This attack was then re-implemented by several researchers, such as Samy Kamkar with his RollJam tool.

KeeLoq itself is also suffering from cryptanalysis attacks like the following:

- Sliding techniques and linear approximation
- Sliding and algebraic method
- Side channels attacks with power analysis

Moreover, after Microchip introduced a seed to improve KeeLoq security, COPACOBANA's parallel computing attack was also published to get required secrets.

Among all these methods to extract the key is another way: dumping the content of the on-chip EEPROM through the in-circuit serial programming (ICSP) if the memory is not read-protected.

There are also interesting services that support many remote types. These would allow an intruder to quickly generate commands from a captured message and see how they can use these to get access.

Opening Doors with Kaiju
Kaiju is a service developed by the creators of PandwaRF, a portable device with a nice form factor that we elaborate on later. This service allows users to send hex or binary payloads to analyze the rolling code of many devices. A complete list of its supported devices is available on the Kaiju project website.

To use the service, we take the hexadecimal of one of the commands we captured and copy it to the form, seen in Figure 23.

![Figure 23. Sending a remote button push to Kaiju](image)

After sending this command, we can successfully decode it and gain useful information that would help us decode the payload we captured.
Figure 2. Remote information from our captured button push

We can see information such as the hexadecimal value that refers to the remote's unique identifier (UID), how the signal is encoded, which button was used, the synchronization counter state, and the cipher algorithm (KeeLoq for this case).

Taking note of the "Sync counter" state, we can now generate the next push of a button on the same page, as seen in Figures 25 and 26.

Figure 25. Generating the next button push rolling code with Kaiju
We need the first part of the rolling code to send it over the air. To do so, we can copy the hexadecimal value to URH. However, natively this will be difficult to do because URH does not seem to take text files in its generator tab. Therefore, to avoid modifying the URH Python code, let us do this on GRC.

On GRC, we take a text file string, unpack bytes into bits, map them to have a mark and a space that consider a 20kHz deviation, (noted earlier when we first captured the signal), and center to DC-Centered to get our 2-FSK final signal. The result is the flowgraph seen in Figure 27.

With this, the receiver should acknowledge the command, allowing us to open the garage with this quick technique. Now, however, we have a different question to ask: What would happen if we mixed the DOR command with the rolling code generation?
Mixing DOR With Rolling Code Brute Force

At this point, Kaiju is not yet available meaning we are not allowed to generate the sixth push of the button as decoded and seen in Figure 28.

![Figure 28. Analyzing a DOR command in Kaiju](image)

After talking to the creators of Kaiju, we learned that the buttons pushed are limited to a value of "4" maximum but this will be unlocked for LEA users, which will prevent every user both from accessing and having permanent access easily.

However since KeeLoq’s implementations are available on the internet, this does not mean the end for our test. Nevertheless, we will still have to encode the payload properly and get the manufacturer key to generate the payload on our own. Furthermore, we will need to identify the chip family and use a PIC ICSP programmer to get the memory, if this memory is not protected on the targeted chip.

Another method that we can use, which would allow us to get a few master keys of other vendors, would be to use the memory dump of the WHY EVO remote, which is based on a STMicroelectronics chip. Afterward, we can interface with this chip through the single wire interface module (SWIM) communication protocol using an ST-LINK/V2 to dump the program and the keys.
Figure 29. The WHY EVO circuit

Figure 30. The pinout of the STM8L151Gx chip
Minimizing the Setup With PandwaRF

Knowing the frequency and the data sent by the remote, we can minimize the setup of an attack using a frequency analyzer with a compact form factor called PandwaRF.

![PandwaRF](image)

Figure 31. The PandwaRF shown close to a remote to see its compact form factor

PandwaRF is indeed an interesting tool in that it can be used by threat actors to conduct stealthy attacks. They would also have to analyze the target as we had done to understand the data we discussed earlier.

Nevertheless, the PandwaRF Android application allows us to see what goes over the air with a proper frequency analyzer that spots the remote sending a command.
Figure 32. The frequency analyzer of the PandwaRF tool showing our remote's signal

It is much more difficult to tell what modulation we are facing using this device, even when zooming in on the signal. However, PandwaRF is still well featured enough to detect it; we just have to follow a few steps to do so. First, we need the right antenna to get enough energy, and then we need to detect the right frequency (+ possible shift). Lastly, we need to force parameters if the auto-measurement fails to capture the data. Following these steps, we can recover what we were able to decode earlier.
After this, we can directly send it to Kaiju because the Android application for this device can connect us directly to this service. Kaiju will then automatically generate rolling codes for us to test. It should be noted that Kaiju also processes incoming data if parameters like the data rate are incorrect on PandwaRF.

Having generated the rolling code, we can send the next commands to the door and open it.

Going back to the DOR command, since PandwaRF allows us to use our own API, we can generate new A and DOR buttons, making it possible to register a new remote to gain permanent access to the mechanism.

**Conclusion**

Through our demonstration, we have shown how it is possible to gain access to a garage door by brute forcing the rolling code of a garage door mechanism. Not only that, but by using the DOR function, we demonstrated how a potential intruder can gain permanent access and proved how a powerful yet compact device such as PandwaRF can make such an attack stealthier to execute.

Cars, garage doors, and Remote Keyless Entry (RKE) systems suffer from not having timestamps when faced with jamming and replay attacks. Looking deeper into the structure of a frame captured over the radio, decoding it, and getting the secrets of its unknown parameters allow attackers to generate codes themselves. Combined with a DOR procedure and similar features in other remotes, attackers need only perform an attack once and then reuse its own recorded remote.
It is only a matter of time before rolling code attacks such as this become a reality that homeowners face. Once an algorithm is known and the master keys are recovered, it would be possible to quickly brute force the remaining parameters within a decent period. Manufacturers, on the other hand, are faced with the challenge to avoid this issue in their own products. They must ensure that their microcontrollers or Secure Elements (SEs) will keep their secrets. In the face of such a possibility, chips must be tested against glitches and side-channel attacks.

**Recommendations**

In order to prevent such an attack from becoming a reality, steps should be taken to make them more complex to execute. This means adding several mechanisms in addition to the rolling code, such as the following:

1. Using a different manufacturer key per remote and introducing diversification so that an attacker would have to find out the generation algorithm of each key, even after dumping the master key
2. Debugging interfaces that are physically disabled on remotes and receivers
3. Implementing memory protection on remotes and receivers to avoid possible leaks
4. Using a seed when adding to the sync counter to complexify the brute-force process

For their part, homeowners can also take steps to prevent such attacks by ensuring that their remote and receivers are secured and adding other security measures. These best practices include:

1. Never leaving open garages unattended for long periods
2. Being mindful of where garage remotes are kept
3. Considering the use of traditional locks such as padlocks and deadlocks to secure garages, especially when one is out of town
4. Installing additional security measures such as sensors and cameras

As this demonstration shows, users should become more mindful of hidden features in their remotes to disable them if necessary. For example, the DOR feature can be manually disabled by removing a jumper on the receiver. Users should also keep the receiver hidden, protected against opening, and strengthened against simple lock-picking attacks.
References


