

An Efficient Security System in Vehicle Using Hooping Code Technique.

Dr.CHANDRA MOHAN

1.PG Scholar 2. Associate Professor

1.revsoft86@gmail.com 2.drvenniraselvi@svcetedu.org

Master of Technology, Sri Venkateswara College of Engineering & Technology, Chittoor, India.

ABSTRACT

More people in the modern world are driving automobiles that have smart key systems, which strengthen the security of the vehicle. The main sorts of attacks and the security of various car types are suggested in this project report. Key fob assaults and deep learning about the Rolling Code attack are the topics that are explored the most in this study. By eliminating the need for a mechanical key and enabling wireless authentication between the car and key fob, this smart key technology makes it easier for drivers to operate automobiles. Although this form of system is more secure, it is still susceptible to attacks like the relay attack, rolljam attack, and jam and sniff attack. Man-in-the-middle attack and replay attack are hacking techniques that are related to relay attack. In a rolljam assault, the attacker listens in on the incoming signal from one side and replays it as needed using a rolljam device. In a jam and sniff attack, the attacker jams the signal between the user's vehicle and himself while simultaneously using an SDR device to record the first and second key presses. The method used to determine whether the signal is coming from the user's smartphone or the attacker's device heavily relies on signal strength. Identifying attacker relay attacks is the primary goal. In this article, we suggest a security method to thwart the aforementioned assaults by utilising 128-bit CBC (Cipher Block Chaining) encryption and decryption between the receiver and transmitter combined with the addition of a real clock that reduces the LoRa signal's maximum validity period. Signal strength needs to be protected because the attacks outlined above rely on its vulnerability. The rolling code signal's time span is limited in this instance so that an attacker in the middle cannot detect it in a timely manner.

Keywords: Cipher Block Chain, LoRa, MIM

I INTRODUCTION

The government required car manufacturers to increase key fob security in the early 1990s. A few years ago, car burglaries took place with the victim's knowledge and a duplicate key from their own set. The installation of RFID immobiliser chips in key fobs is the first attempt at an automotive security solution. Immobilizer alarms were first made available by St. George Evans in 1919 by the manufacturers to secure the car hacks. After that, in 1995, a wide range of auto manufacturers began to create and construct cars with immobiliser chips. From January 1, 1998 in Germany and January 2007, in Canada, immobilisers gained popularity and were mandated for all new vehicles. After the immobiliser chips were installed in key keys, there was a greater decrease in automobile theft activity. Since automakers have become experts at incorporating more technology and software for security purposes, thieves have gotten better at knowing how to circumvent technology so that cars can be stolen using keys.

The remote unlocking of a modern automobile with a key fob is very common. Renault debuted the radio-frequency identification (RFID) keyless entry technology in 1982, which was successful in the market for the following 10 years. There, the foundation for the security features was laid. The key fobs can then be accessible by recording the infrared light source that was introduced with the infrared technology. All automobile manufacturers had previously begun using RFID signals in key fobs to unlock doors and start cars. The key fob

transponder's frequency range was 125 kHz. A signal from one end is required for this range to connect with the sender and receiver, which secures the car by starting.

We will investigate how remote key fobs, which are used to open and start vehicles, set up remote interchanges, using SDR devices. Most modern frameworks rely on a moving code or test reaction framework, which prevents simply recording and playing back a fixed code by prodding the critical fob to play out an assignment, like finishing an estimation and returning the correct answer. While more established key fobs use a straightforward fixed code to start the vehicle, most modern frameworks rely on moving codes or test reaction frameworks.

Radio-Frequency Identification, or RFID, is a wireless technology that uses tiny devices to transmit IDs to RFID readers. An RFID tag called EPC (Electronic Product Code) is most frequently utilised in supply chains. Data is transmitted from RFID tags to an antenna/reader combo via radio waves. The chip is activated by this type of energy, which activates the energy, and the signal is transmitted via the antenna.

RFID encompasses immobilisers. When it first started, it didn't offer security, but today it does. The vehicle theft can be investigated using an RFID transponder by turning on the engine injection system of the car. Later, the manufacturers gained further security by integrating RFID signals into the engine start. User access to it is dependent on the signal.

A radio device called the RollJam (Figure 1) has a significant influence on keyless entry systems, door openers, and alarm systems that are made to decipher rolling codes. The RollJam device is positioned within the car or garage's shortest distance. The attacker can access the victim's key when they use it to send a signal. The key fob won't function the first time, but the second time it will either lock or open it. The user is prevented from unlocking the door by this device, which makes them believe they have a contact once more. It stores the original signal from the user's key fob. The user then taps the key fob once more. The RollJam records the second code, jams, and broadcasts the first code on the second press, which unlocks the door. The key benefit of a RollJam attack is that the perpetrator can replay the user-captured code and use the intercepted signal to unlock the vehicle. Any high-end vehicle can be used to test this attack.

The attacker attempts to use a jammer device to disrupt the signal that occurs between the car and the key, according to the Jam and Sniff attack. The attacker clogs the signal when users press the key. The attacker uses a certain SDR device at the same time to try and sniff the signal. In this scenario, the user continues to turn the key until the automobile is shut. On the other side, the attacker intercepts many signals by sniffing them, then repeats the first signal that was intercepted when the jammer device is disabled. Although the attacker has the opportunity to replicate the signal, the car is locked. This is the most current attack that takes place in a vehicle that uses the rolling code concept.

Since the key fob cannot transmit at a precise frequency, these estimates need a lot of power and battery utilisation. Higher frequency is required by the key fob for long-distance communication. Consequently, the battery needs to be more powerful for long-distance communication.

The key fob typically transmits an ID and a counter for how many times a key has been pressed. This information is encrypted and transferred to the automobile when you click the button. An method is used to change the starting number (let's call it x) to the following number in the series ($x+1$), once the remote and computer are synchronised.



Fig 1 RollJam device

II LITERATURE SURVEY

In their presentation, Jinita Pate, Manik Lal Das, and Sukumar Nandi [1] discussed the advancement of the RKE system as well as improvements to encryption and decryption that prevent hackers from mistaking the secure procedure. The RKE device allows for eavesdropping, relay, replay, on-board diagnostic (OBD) port scan, key fob duplication, jamming, and other assaults. In this paper, they discuss keyless car entry systems, point out many security holes in a current RKE system, and suggest a new RKE method. Their conclusion, which leads to a good solution, states that the fundamental RKE system is vulnerable to OBD port attack. As a way to improve security in the Smart Key system, Madhumitha Sri Selvakumar, Rohini Purushothkumar, Arunkumar Ramakrishnan, and Gunasekaran Raja [3] presented an approach. The car is protected from replay attacks using the Keeloq algorithm and the Play Fair cypher technology, which also automatically eliminates communication-related threats. Keeloq is the algorithm used the most in Keyless Entry systems This paper suggests the idea of rolling code. The authors presented efficient cryptography with the RKE Crypto model, which is vulnerable to a significant replay attack. The communication attack on the RKE system is also lessened. When using the rolling code notion, an algorithm is employed to change the starting number (let's call it x) to the following number in the series $(x+1)$.

A solution for securing a car remote keyless entry system was put forth by Patrick DeRoy and Andreas Barchanski [4]. The Bulk Current Injection test is an extremely repeatable and simple setup. The range of frequencies is 15 MHz to 30 MHz. By conducting several attacks on it, the authors are primarily interested in the functionality of the RKE (Remote Keyless Entry) technology. The receiver side of the remote keyless entry system, which is put through a bulk current injection test, exhibits the RF immunity non-compliance. The result (Measurements and simulations) indicates the harmonics are introduced in the frequency passband on the receiver side of 314.9 MHz as high as 30 dB, which was above the typical key fob signal levels.

Using symmetric key cryptography, Tobias Glocker and Timo Mantere [5] proposed a technique for securing a vehicle's remote keyless entry system. This protocol, which secures the vehicle against attacks like the Two-Thief attack, is suggested by a lightweight symmetric encryption method. The security mechanism should improve as the comfort level of the oncoming car rises. It is unlikely that a vehicle may be compromised using this protocol. The system needs more energy to overcome the lightweight encryption

OVERVIEW OF KEYS AND THE ATTACKS

DENOMINATION	ENTRY	START ENGINE
Physical Key	Physical Key	Physical Key
Physical Key with Immobilizer	Physical Key	Physical Key +RFID
Remote Keyless Entry System	Remote active (press button)	Physical Key +RFID
Remote Keyless Ignition System	Remote passive	Remote passive

TABLE 1 shows the different types of key and their access

TYPES OF ATTACKS

Attackers frequently target both new and vintage autos in their attacks. Rolling code and implementing the report can stop the following attacks.

RADIO JAMMING ATTACK

The car is unlocked or locked in this extremely straightforward assault by blocking the locking signal from the key, as demonstrated in Fig 2. An attacker only needs a radio transmitter to send junk code at the same frequency to block the communication. The attacker must be close enough to the car to be able to block the signal, thus that's what's vital. The attacker in this attack can take the car, but they are unable to start the engine. To ensure that the automobile is either locked or unlocked, all cars are equipped with a specific sound and flashing light for this purpose, undermining the attack.

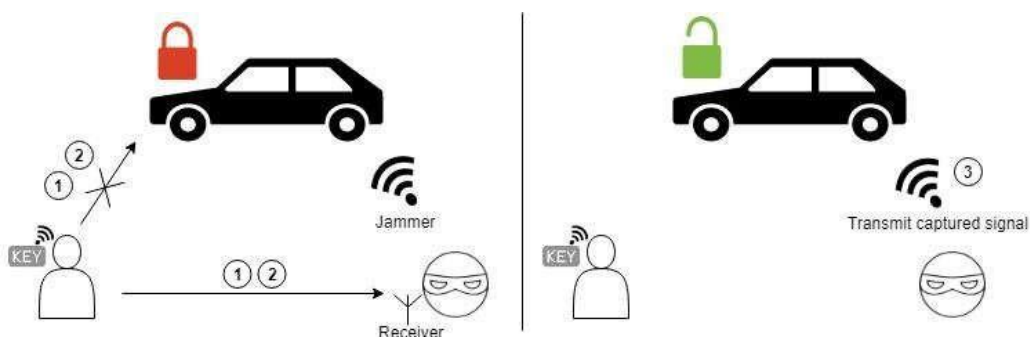


Fig 2 Radio Jam Attack

ROLLJAM ATTACK

The keyless entry system, door opening system, and alarm system that are intended to interpret rolling codes are greatly impacted by the RollJam, a radio device. Within the car or garage, the Rolljam device is put in the area with the shortest range. The attacker can access the signal when the victim uses it to transmit one. The key lab will network the first time; however, the second time, it will either lock or unlock. This gadget keeps a copy of the initial sign from the user's key lab and prompts the user to unlock the door, making them think they need to make another contact. A second key fob push is made by the user. The RollJam jams and broadcasts the first code after recording the second code on the second press, unblocking the door. The primary benefit of a RollJam attack is that it allows the attacker to unlock the vehicle by replaying the user-captured code and signal. Any expensive car can be used to test this attack.

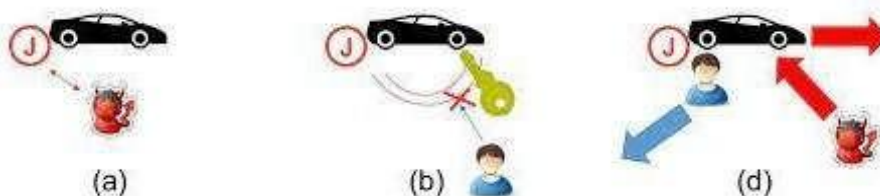


Fig 3 RollJam Attack

RELAY OVER CABLE ATTACK

Two antennas that generate an LF signal are used in the relay over-cable assault, and the cables are linked together. The amplifier is placed in the middle to enhance the sign between the assailant and the vehicle. The loop antenna are positioned next to the vehicle door, creating the local magnetic field that picks up the automobile beacon signal. The second antenna will receive the electrical signal through the coaxial connection, which immediately creates a magnetic field. The initial messages from the car will be picked up by the magnetic field.

The attacker's job is now relatively straightforward; all he needs is for the relaying antenna to be close to the door in order to deliver the open signal that aids in starting the engine.

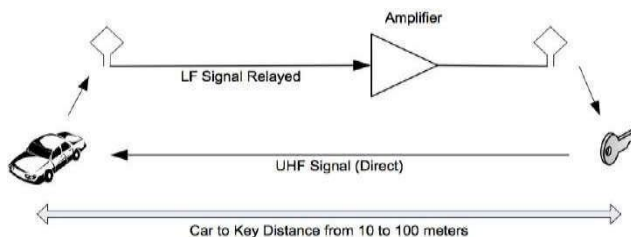


Fig 4 Relay over Cable Attack

GETTING THE REACTION CODE FROM MEMORY

There is a potential that the immobilizer's memory could receive a response code after the key fob receives a signal. Key fob must be stopped from propagating signals in order to find this. By doing this, the attacker gains access to the vehicle through a window created by the key fob's signal sniffing and the signal to the immobilizer memory remaining inactive. If the attacker is able to pinpoint the memory that stores the information, it will be simple for them to gain access to the car. In this scenario, the attacker may even be able to record data from a particular memory.

BRUTE FORCING A KEY CODE

According to the key code length and algorithm of the code, the brute force method helps to access the response code through feasibility of brute force attack. There is a specific cryptography called Immobilizer Cryptography plays major role in key system security. This attack is so simple as using a SDR device with the related software. Software like gqrx helps to active the brute force attack.

Combination of hardware (SDR) and software (gqrx) will leads to simple brute force attack. In some case, the key fob may detect the attack. In these case, custom hardware reset is required for improving the power for the lockout.

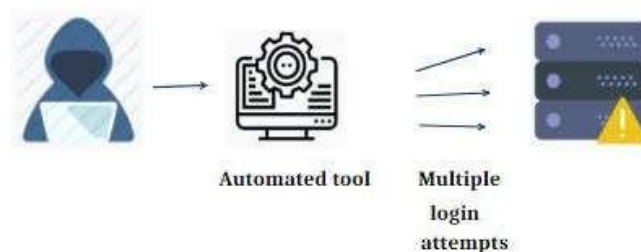


Fig 5 Brute Force Attack

RELAY OVER THE AIR ATTACK

Because LF signal emission in a relay-over-the-air attack occurs with less delay than in a relay-over-cable attack, it is preferred over the latter. The RF link is being constructed with the help of delayed emission. When the LF signal is amplified, it travels to the emitter and changes to 2.5 GHz where air serves as the transmission medium. To obtain the dynamic LF signal, the receiver transforms the received signal according to its intended use.

The LF signal can be amplified and prospected to an LF loop antenna to reproduce the signal.

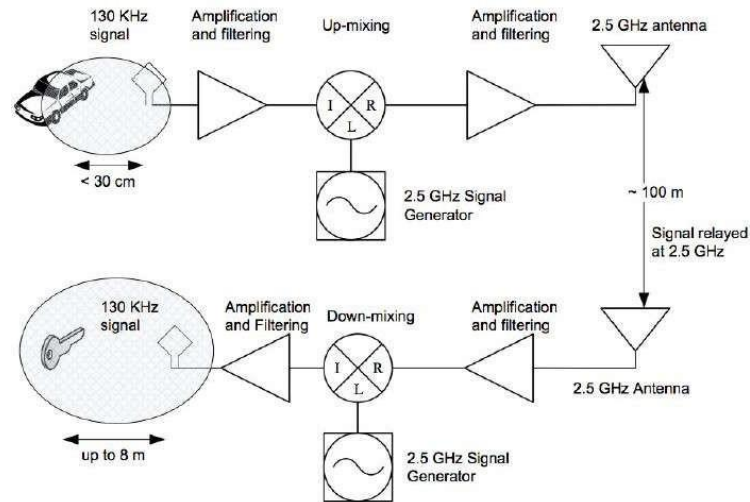


Fig 6 Relay over the air attack

ATTACKING A PKES SYSTEM

The range of frequencies is 15 MHz to 30 MHz. By conducting several attacks on it, the attackers are primarily concerned with the functionality of the RKE (Remote Keyless Entry) technology. Bulk Current Injection, or BCI, is a notion that quantifies how well a system performs within a given frequency range of 15MHz to 30MHz. The BCI exam causes the frequency spectrum to change. The standard frequency band has a 106 dBA level. On an RKE system, the authors ran this BCI test. Since the bulk current injects the system, this frequency causes failure in the RKE system. Since the injected waveform is nonlinear, the sinusoidal current waveform impacts the frequency of 106 and causes the RKE electronics to rise to undesirable harmonics on the receiver side. Experimental measures are evaluated using computational electromagnetic simulation to confirm the results. The authors suggested a robust way to determine whether the system is actually congested and is of poor quality. With this technique, it is no longer necessary for the attacker to approach the key in order to start the relay process. For security reasons, keyless entry for vehicles was introduced to replace mechanical keys. Although it does not completely guarantee security, the remote keyless entry technology enhances vehicle security. two effective wired and wireless physical layer relays were used to demonstrate a relay assault on the Passive Keyless Entry and Start (PKES) system.

This idea enables the attacker to hack the vehicle and get inside. By transmitting the signal between the car and the car key, the attacker can even start a car. Relays offered here are free from strict authentication requirements, protocols, and encrypted modulation. The author discovered through this assault that there is only one direction in which the relaying signal can be conveyed.

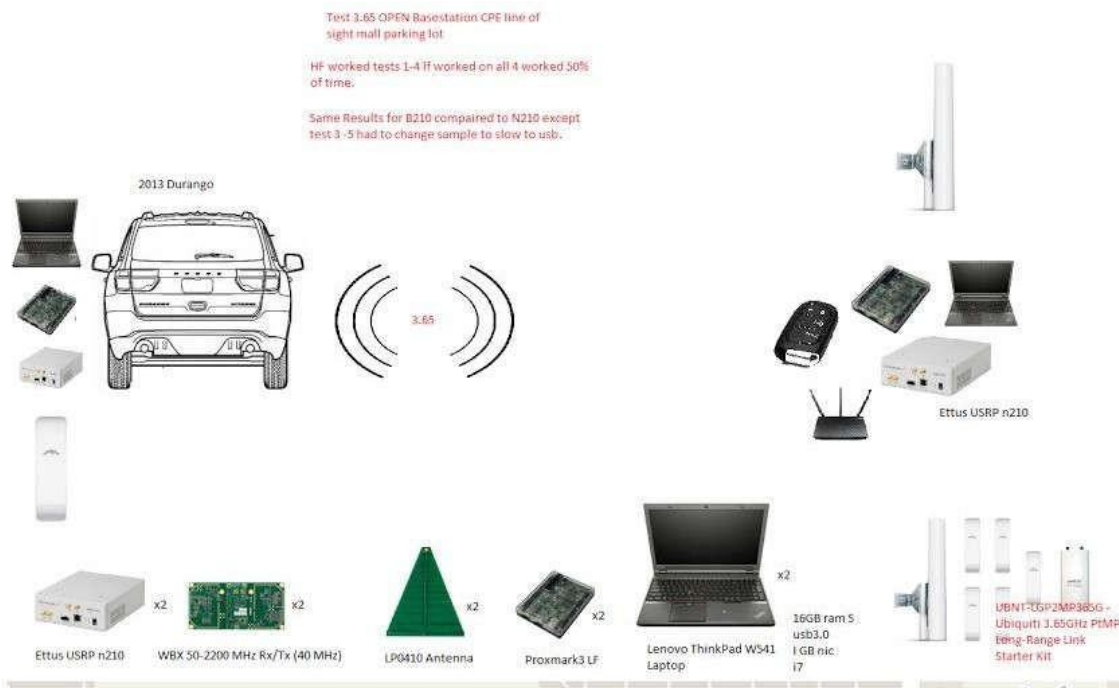


Fig 7 PKES System

The security mechanism should improve as the comfort level of the oncoming car rises. The most common comfort in a car is safety. Security features heavily rely on cryptography. Cryptography is necessary for both wired and wireless devices. This study describes potential Remote Keyless Entry system assaults and suggests a safe procedure or policy using a portable symmetric encryption technique.

ELECTRONICS ATTACKS

Encryption and Decryption Attacks

The cryptographic calculations to use the remote key passing frameworks have been the subject of more research. The Keeloq computation is one of the calculations in use. Short keys, which the network has openly overlooked with shoddy encryption computations, are frequently the cause of suspected assaults. Producers are moving toward stable, prosperous, and working figures as a result. Transfer assault is independent of the character used; it doesn't require knowledge of or command over the information to operate.

Jamming attack

Use of a simple jammer is a notable attack against keyless vehicle opening frameworks. When the user immediately steps down, he will press the key fob to lock the car. In this scenario, the user-sending signal will be interfered with, resulting in the vehicle's continued unlocking. In the event that the owner of the vehicle missed the fact that it didn't bolt, the fraudster will be able to approach the vehicle. The jammer can keep the car unlocked but it cannot be used to start the engine. To unlock the car, another technique is to record the signal and play it back against it. A counter will be used in standard cryptographic operations like encryption and decryption to guard against replay sniping.

Electronics Parts

Electronic parts providers give segments to detached keyless section frameworks, those segments are then utilized by different vehicle producers. In spite of the fact that varieties exist in the conventions and cryptographic obstructs, all makers give frameworks dependent on the equivalent joined LF/UHF radio innovation. Therefore, the attack we have presented is likely to have an impact on such frameworks.

Keyless system attacks

The Keyless Car Entry systems are secured by the designers against hand-off attacks. The detailed hand-off attack consists of two separate UHF hand-off connections to hand-off messages in the two bearings. The proven evaluation recognizes the transfer issue. The problem with the suggested novel arrangement is that it creates an input circle because the vehicle will also get the transferred signal from the next connection. We demonstrate that such an acknowledgment is not necessary in current PKES frameworks and provisionally exhibit it. Additionally, neither a hardware plan nor a realistic execution of the assault is provided by the authors. Finally, no satisfactory outcomes are carried out, and this results in no countermeasure. However, there is no detailed information available, and it is unrealistic to expect to understand the specifics of the assault. It is unclear if the assault relies on a hand-off at the physical layer or on an adjustment/demodulation transfer. Additionally, it is challenging to determine from detailed facts whether an assault actually occurred.

PROPOSED

Aim to build a prototype that can fend off rolling code attacks. In this CBC (Cipher Block Chaining) prototype, signal/code theft against a potent SDR like HackRF is avoided via encryption and decryption. The primary goal is to shorten the period of communication between the automobile and car key within a particular range. The key fob typically delivers an ID and a count of how many times a key has been depressed in addition to an ID. This data is encrypted and transferred to the car when the button is pressed. The first number in the series (let's call it x) is converted to the next number in the series ($x+1$) using an algorithm after the remote and computer are synchronised.

Sending erroneous data into the RFID receiver is another method of jamming the key fob signal. There is room to listen to the passband, or specialised RFID receiver signal. The passband has a few blank spaces (width) that can take useless data. In order to stop attackers from altering the rolling code signal, that window actually has to fill up with noise.

III METHODOLOGY

Vehicles now come equipped with more advanced technologies, but attacks on vehicles are also rising. Artificial intelligence is used to implement self-driving features because cars are connected to the internet. Attackers continue to devise new ways to eliminate these features. These features are designed to be secure and convenient for users. But these characteristics also carry a risk, giving the attacker access. Transponder technology is used in key fobs to carry signals from the key fob to the vehicle, enabling safety features like locking and unlocking doors and starting engines. The key fob and vehicle are well connected when the immobilizer and signal from the fob come into touch, allowing the vehicle to receive the command to carry out the required functions.

Initial key fobs are simply used to operate locks and unlock doors. Since the attacker is not always visible, just one code will be produced. The manufacturers began to improve the code, and today each time a press is used, a new code (a rolling code) is generated that is more secure than the previous one. The new generating code is already in sync with the rolling code.

The key fob typically delivers an ID and a count of how many times a key has been depressed in addition to an ID. This data is encrypted and transferred to the car when the button is pressed. The first value in the series (let's call it x) is converted to the next number in the series ($x+1$) using an algorithm once the remote and computer are synchronised.

RELAY ATTACK

A SDR device called HackRF is used to carry out the replay attack against the car key fob. One gadget is employed. An application called gqrx from the Kali Linux OS is used to capture and recognise the signal and frequency. The signal will be captured using the SDR, shown in gqrx, and delivered to the GNU radio companion programme.

The GNU Companion application listens to signals with a similar flow. Once the user pushes the key fob, the signal is recorded and saved in GNU for later use.

To carry out more relay attacks on the targeted car, the collected data are sent to the HackRF-SDR device. The attacker will then have access to the desired vehicle.

SECURITY METHODS FOR RELAY ATTACK SECURITY

The earliest and most basic method was to record and then replay the waveform that a key fob emits (HackRF). However, some vehicles still have key fobs that operate in this manner and are vulnerable to assault (some pre-2000 Mercedes for example). Replay attacks are suggested for vehicles that employ rolling keys. When the key fob is not in the car, the attacker can replay the signals they have recorded and record several key strokes to unlock the vehicle.

The victim's key fob's output is recorded in the second attempt to unlock the vehicle, which also jams the vehicle. Attacking a key fob often involves analysing the transmission from the key fob and then jamming it when signals are sent to the other end. By using this method, the packets being transferred from one end to the other cannot be identified, but the signal can be recorded and then converted into a waveform.

Last but not least, a jammer on its own will prevent the remote from working to lock the car. If the motorist is not paying attention, they can leave the car open as they leave.

ROLLING CODE ATTACK

The concept of rolling codes was discovered to stop the attacks discussed in Chapter 2 above. The key fob typically transmits an ID and a counter for how many times a key has been pressed. This information is encrypted and transferred to the automobile when you click the button. An algorithm is utilised to change the initial number (let's call it x) to the following number in the series ($x+1$), once the remote and computer are in sync. The figure below provides a full explanation of the idea.

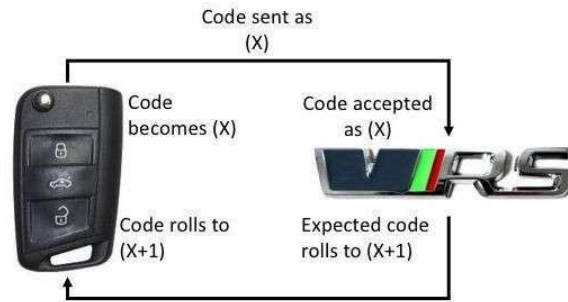


Fig 8 Rolling Code Method

This procedure will aid in preventing the relay attack, which occurs when the codes for one response differ from the next. Whenever a fresh code or signal is produced and recognised by the transponder on the other side. This has the effect of allowing the attacker in the middle to sniff the signal or code but preventing them from using it for other purposes.

SECURITY METHODS ON ROLLING CODE ATTACK

As the Rolling Code emerged as a novel idea in the realm of automobile production, hackers began to target it. The entire vehicle was the target of the rolling code attack known as Jam and Sniff. Jam and Sniff attacks are easily carried out with a few pieces of gear. The middle attacker placed the jammer in close proximity to the targeted car. The attacker in the middle clogs the signal when the user wants to send it, i.e. tries to close the automobile. This prompts the user to attempt again until wireless communication allows the vehicle to close. Keys have been pressed repeatedly.

The attacker grabs the signal using an SDR device like HackRf (shown in the below diagram), etc., and all the signal/code corresponds to the number of key presses. The attacker now disables the jammer and plays the first signal or code that he has taken. HackRF is an SDR device that can send and receive radio signals between 1MHz and 6MHz. To communicate more widely, it converts a signal from digital to radio waveform format. Its purpose is to evaluate, create, improvise, and change current radio frequency systems. Simply put, a software-defined radio is a radio communication device in which software is used rather than conventionally constructed hardware (these would include mixers, amps, and modulators for example).

Radio waveforms are transformed in SDR via digital signal processing. It reminds me of the well-liked software-based digital audio techniques from a few decades ago. Just like a sound card in a computer digitises audio waveforms, a software radio peripheral does the same for radio waveforms. The speaker and microphone have been replaced with an antenna, making it essentially a high-speed sound card. In a small, portable package around the size of a cell phone, the HackRF One is an all-in-one SDR. The user now understands that the car is closed. The next signal or code is, however, already in the attacker's possession through the idea of sniffing. The next signal or code can now be replayed by the assailant to access the vehicle or unlock it. This assault got going quickly and responds to the environment like a typical key fob attack.



Fig 9 SDR Device (HackRF One)

Requirement Analysis

S.No	MATERIALS	QTY
1	Arduino Uno	2
2	LoRa sensor	2
3	Push button	1
4	LED display	2
5	Output devices	req
6	Batteries	req
7	Connecting wires	req
8	Tester switch	1

Any functioning device (such as LED lights, a viper, or a motor) for this prototype can serve as the output device in this scenario. The Arduino performs the same functions as IC (Integrated Circuit) chips in a car. In this prototype, a medium with an operating system is preferred. In a vehicle, all IC chips are coupled to a BUS/CAN protocol.

In a car, the LED screens serve as both the key fob and the transponder. It serves as both the sender and receiver's output screen and displays the function that runs through the procedure.

The LoRa (LoRa Series Ra-02 Spread Spectrum Wireless Module) RF module has a voltage range of 20 dBm to 100 mW and a high sensitivity range of -148 dBm. Communication is two-way.

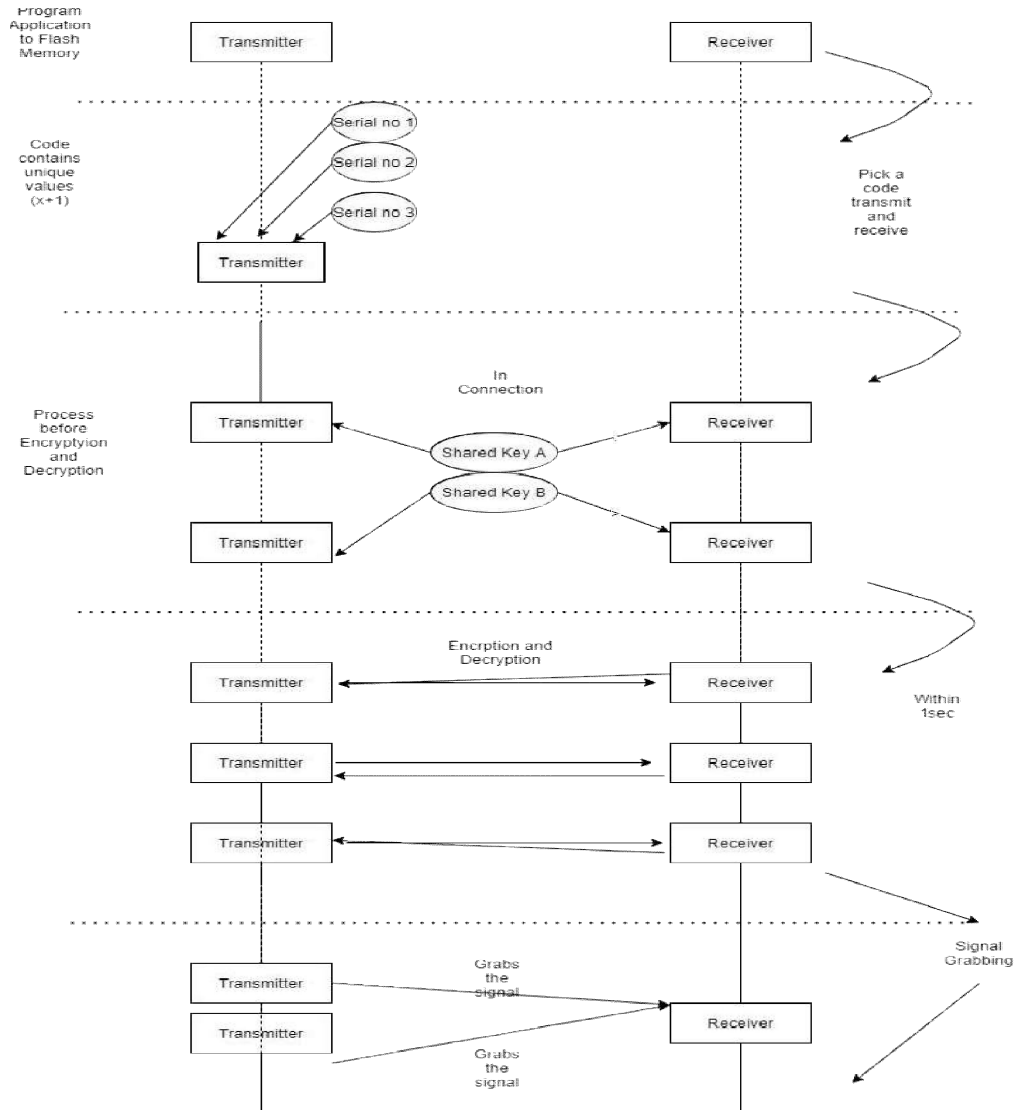


Fig 10 Architecture of prototype model.

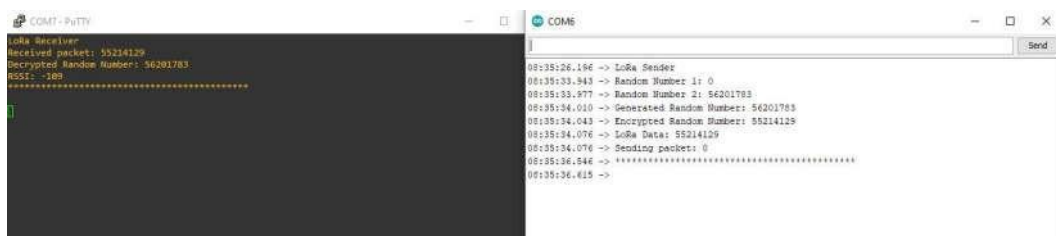
Usually, the key fob communicates an ID and a counter for how many times a key has been depressed along with an ID. When you press the button, an encrypted version of this is sent to the vehicle. Once the remote and device are synchronised, an algorithm is used to take the first number in the series (let's call it x) and change it to the second number (x+1).

The programmed transmitter and sender are parallel to one another, according the architecture (fig). There are more than two serial ports on the transmitter's one side. There are three serial ports in our situation. These ports specify the signal or code that will be captured in the near or far future. The transmitter needs ports for the decryption because rolling codes are designed to work with numerous fresh signals and codes. The receiver only receives one signal or code at a time in this architecture. The same signal or code cannot be used again in the subsequent instance. For access, the sender therefore possesses the ideal decryption technique. When the key or signal is matched by the encryption and decryption processes, this transmitter and receiver are connected.

128 CBC methods are used in encryption and decryption to cut down on signal span time. The assault occurs due to the present valid signal or code's lag in time, per standard rolling coding. When you press the button, an encrypted version of this is sent to the vehicle. Once the remote and device are synchronised, the encryption and decryption procedure starts with the first number and moves on to the subsequent numbers using a 128 bit CBC technique.

IV RESULTS

The transmitter and receiver link in accordance with the implementation, producing the desired outcomes. The sender tries to connect with the receiver in the graphic below, and the results reveal that encryption and decryption have occurred, but the range value is higher than the mid-range. Hence the door is locked.



```

COM1-PUTTY
LoRa Receiver
Received packet: 55214129
Decrypted Random Number: 56201783
RSSI: -109
*****

COM6
00:35:36.196 -> LoRa Sender
00:35:33.943 -> Random Number 1: 0
00:35:33.977 -> Random Number 2: 56201783
00:35:34.010 -> Generated Random Number: 56201783
00:35:34.043 -> Encrypted Random Number: 55214129
00:35:34.076 -> LoRa Data: 55214129
00:35:34.076 -> Sending packet: 0
00:35:36.546 -> *****
00:35:36.615 ->

```

Fig 11 Result 1

The results of the sender and receiver reconnecting reveal that encryption and decryption have occurred, however the range values are over the mid-range in the image below. Given that the LoRa RF module provides a high level of connectivity over a small distance, range is particularly crucial in this approach. The door is therefore secured.



```

LoRa Receiver
Received packet: 55214129
Decrypted Random Number: 56201783
RSSI: -109
*****

Received packet: 53164194
Decrypted Random Number: 54151848
RSSI: -100
*****

COM6
00:35:36.196 -> LoRa Sender
00:35:33.943 -> Random Number 1: 0
00:35:33.977 -> Random Number 2: 56201783
00:35:34.010 -> Generated Random Number: 56201783
00:35:34.043 -> Encrypted Random Number: 55214129
00:35:34.076 -> LoRa Data: 55214129
00:35:34.076 -> Sending packet: 0
00:35:36.546 -> *****
00:35:36.615 ->
00:37:10.506 -> Random Number 1: 0
00:37:10.541 -> Random Number 2: 54151848
00:37:10.574 -> Generated Random Number: 54151848
00:37:10.607 -> Encrypted Random Number: 53164194
00:37:10.641 -> LoRa Data: 53164194
00:37:10.641 -> Sending packet: 1
00:37:13.128 -> *****
00:37:13.163 ->

```

Fig 12 Result 2

The sender tries to connect with the receiver once more in the graphic diagram is given below, and the results reveal that encryption and decryption have occurred, but the range values are below the mid-range. The transmitter and receiver are connected when the car key and the transponder are matched because the range in this situation does not exceed the mid range. The door thusly opened.

```

Received packet: 68485815
Decrypted Random Number: 69473469
RSSI: -110
*****
Received packet: 38412704
Decrypted Random Number: 39400358
RSSI: -110
*****
Received packet: 38279954
Decrypted Random Number: 39207608
RSSI: -110
*****
08:37:56.550 ->
08:38:04.090 -> Random Number 1: 0
08:38:04.124 -> Random Number 2: 69473469
08:38:04.124 -> Generated Random Number: 69473469
08:38:04.151 -> Encrypted Random Number: 68485815
08:38:04.224 -> LoRa Data: 68485815
08:38:04.224 -> Sending packet: 3
08:38:06.697 -> *****
08:38:06.765 ->
08:38:16.952 -> Random Number 1: 39400358
08:38:16.966 -> Random Number 2: 0
08:38:17.020 -> Generated Random Number: 39400358
08:38:17.055 -> Encrypted Random Number: 38412704
08:38:17.069 -> LoRa Data: 38412704
08:38:17.069 -> Sending packet: 4
08:38:19.573 -> *****
08:38:19.607 ->
08:38:32.736 -> Random Number 1: 39207608
08:38:32.771 -> Random Number 2: 0
08:38:32.771 -> Generated Random Number: 39207608
08:38:32.805 -> Encrypted Random Number: 38279954
08:38:32.840 -> LoRa Data: 38279954
08:38:32.875 -> Sending packet: 5
08:38:35.333 -> *****
08:38:35.403 ->

```

Fig 13 Result 3

V CONCLUSION

With this prototype, the security against a rolling code attack is defined. Although this prototype may not provide a precise answer, it does provide a general framework for rolling code attack protection. The same prototype may be altered to function as a system in a car. For security reasons, this system is easily connected to the CAN BUS protocol. Although the use and development of RFID in car keys has reduced auto theft, the attackers are also expanding and target vehicles that have a slight functional flaw. The consumers should be aware of how to secure their car from an attacker even though the manufacturers offer new secure safety. Even though various types of assaults are described, the key fob's security is not up to par. Key fobs are very insecure, which encourages attackers to attack them, gain access to them, and start the vehicle.

This prototype has a shorter duration between the sender and the receiver for which the signal intensity can be communicated. The communication procedure will occur in under one second. This prevents the attacker from intercepting the middle signal.

REFERENCE

- [1] J. Patel, M. L. Das and S. Nandi, "On the Security of Remote Key Less Entry for Vehicles," 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, IEEE 2018.
- [2] S. van de Beek, R. Vogt-Ardatjew and F. Leferink, "Robustness of remote keyless entry systems to intentional electromagnetic interference," 2014 International Symposium on Electromagnetic Compatibility, pp. 1242-1245, IEEE 2014.
- [3] M. S. Selvakumar, R. Purushothkumar, A. Ramakrishnan and G. Raja, "Effective Cryptography Mechanism for Enhancing Security in Smart Key System," 2018 Tenth International Conference on Advanced Computing (ICoAC),pp. 190-195,IEEE 2018.
- [4] P. DeRoy et al., "Bulk current injection assessment of automotive remote keyless entry systems," 2017 IEEE International Symposium on Electromagnetic Compatibility & Signal/Power Integrity (EMCSI),pp. 660- 664,IEEE 2017.

- [5] T. Glocker, T. Mantere and M. Elmusrati, "A protocol for a secure remote keyless entry system applicable in vehicles using symmetric-key cryptography," 2017 8th International Conference on Information and Communication Systems (ICICS),pp. 310-315,IEEE 2017.
- [6] J. Wang, K. Lounis and m. zulkernine, "cskes: a context-based secure keyless entry system," 2019 IEEE 43rd Annual Computer Software and Applications Conference (Compsac), Milwaukee,pp. 817-822,IEEE 2019.
- [7] T. Yang, L.Kong, w. xin, j. hu and z. chen, "resisting relay attacks on vehicular passive keyless entry and start systems," 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery,pp. 2232-2236,IEEE 2012.
- [8] M. k. Roy and t. fleissner, "rf performance optimization of a saw based transmitter for remote keyless entry system," 1994 Proceedings of IEEE Ultrasonics Symposium,pp. 169-173 vol.1,IEEE.
- [9] S. van de Beek and F. Leferink, "vulnerability of remote keyless-entry systems against pulsed electromagnetic interference and possible improvements," in IEEE Transactions on Electromagnetic Compatibility, vol. 58, no. 4, pp. 1259-1265,IEEE 2016.
- [10] O. Alaca, A. Boyaci, S. Yarkan and m. a. aydn, "a statistical modulation type identifier for remote keyless entry transmitters based on extended energy detector," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos,pp. 1-6,IEEE 2019
- [11] ATMEL. e5561 Standard Read/Write Crypto Identification IC, 2006. datasheet,available <http://www.usmartcards.com/media/downloads/366/Atmel%20e5561%20pdf-190.pdf>.
- [12] ATMEL. Embedded AVR Microcontroller Including RF Transmitter and Immobilizer LF Functionality for Remote Keyless Entry - ATA5795C. datasheet, available at http://www.atmel.com/images/Atmel-9182-Car-Access-ATA5795C_Datasheet.pdf, November 2014.
- [13] Bloessl, B. gr-keyfob. Github repository, 2015. <https://github.com/bastibl/gr-keyfob> Bogdanov, A. Attacks on the Kee-Loq Block Cipher and Authentication Systems. In Workshop on RFID Security (RFIDSec' 08) (2007). rfidsec07.etsit.uma.es/slides/papers/paper-22.pdf.

- [14] Bono, S. C., Green, M., Stubblefield, A., Juels, A., Rubin, A. D., and Szydlo, M. Security analysis of a cryptographically-enabled RFID device. In 14th USENIX Security Symposium (USENIX Security 2005) (2005), USENIX Association, pp. 1–16.
- [15] Cesare, S. Breaking the security of physical devices. Presentation at Blackhat'14, August 2014. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S.,
- [16] Koscher, K., Czeskis, A., Roesner, F., and Kohno, T. Comprehensive experimental analyses of automotive attack surfaces. In 20th USENIX Security Symposium (USENIX Security 2011) (2011), USENIX Association, pp. 77– 92.
- [17] Courtois, N. T., O'Neil, S., and Quisquater, J.-J. Practical algebraic attacks on the Hitag2 stream cipher. In 12th Information Security Conference (ISC 2009) (2009), vol. 5735 of Lecture Notes in Computer Science, Springer-Verlag, pp. 167–176.
- [18] Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., and Shalmani, M. T. M. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In Advances in Cryptology – CRYPTO'08 (2008), vol. 5157 of LNCS, Springer, pp. 203– 220.
- [19] Francillon, A., Danev, B., and Capkun, S. Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of the Network and Distributed System Security Symposium, NDSS 2011 (2011), The Internet Society.
- [20] Indestege, S., Keller, N., Dunkelman, O., Biham, E., and Preneel, B. A practical attack on KeeLoq. In 27th International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT 2008) (2008), vol. 4965 of Lecture Notes in Computer Science, Springer- Verlag, pp. 1–8.
- [21] Kasper, M., Kasper, T., Moradi, A., and Paar, C. Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed. In Progress in Cryptology - AFRICACRYPT'09 (2009), B. Preneel, Ed., vol. 5580 of LNCS, Springer, pp. 403–420.
- [22] Kasper, T., Oswald, D., and Paar, C. Wireless security threats: Eavesdropping and detecting of active RFIDs and remote controls in the wild. In 19th International Conference on Software, Telecommunications and Computer Networks – SoftCOM'11 (2011), pp. 1–6.

- [23] Keyline S.p.A. RK60 guide, 2015. Available at http://www.keyline.it/files/teste-elettroniche/electronic_heads_guide_13316.pdf.
- [24] E. Nickel, "IBM automotive software foundry," in Proc. Conf. Comput. Sci. Autom. Ind., Frankfurt, Germany, 2003.
- [25] M. Wolf, A. Weimerskirch, and T. Wollinger, "State of the art: Embedding security in vehicles," EURASIP J. Embedded Syst., vol. 2007, no. 5, p. 1, 2007.
- [26] R. Charette, This Car Runs on Code. [Online]. Available: <http://www.spectrum.ieee.org/feb09/7649>
- [27] T. Nolte, H. Hansson, and L. L. Bello, "Automotive communications-past, current and future," in Proc. IEEE Int. Conf. Emerging Technol. Factory Autom., 2005, vol. 1, pp. 992–999.
- [28] K. H. Johansson, M. Torngren, and L. Nielsen, "Vehicle applications of controller area network," in Handbook of Networked and Embedded Control Systems. New York, NY, USA: Springer-Verlag, 2005, pp. 741–765.
- [29] T. Hoppe and J. Dittman, "Sniffing/replay attacks on CAN buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy," in Proc. Conf. Embedded Syst. Security, 2007, pp. 1–6.
- [30] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures," Rel. Eng. Syst. Safety, vol. 96, no. 1, pp. 11–25, Jan. 2011.
- [31] K. Koscher et al., "Experimental security analysis of a modern automobile," in Proc. IEEE Security Privacy. Symp., Oakland, CA, USA, 2010, pp. 447–462.
- [32] The EVITA project, 2008, Webpage. [Online]. Available: <http://evita-project.org>
H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, and D. Scheuermann, "Car2X communication: Securing the last meter—A cost-effective approach for ensuring trust in Car2X applications using in-vehicle symmetric cryptography," in Proc. Conf. Veh. Technol., San Francisco, CA, USA, 2011, pp. 1–5.
- [33] H. Schweppe et al., "Securing Car2X applications with effective hardware software codesign for vehicular on-board networks," in Proc. Conf. Autom. Security, Berlin, Germany, 2011.

- [34] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Efficient in-vehicle delayed data authentication based on compound message authentication codes," in Proc. Conf. IEEE 68th Int. Conf. Veh. Technol., Calgary, BC, Canada, 2008, pp. 1–5.
- [35] B. Groza and S. Murvay, "Efficient protocols for secure broadcast in controller area networks," IEEE Trans. Ind. Informa., vol. 9, no. 4, pp. 2034–2042, Nov. 2013.
- [36] C. W. Lin and A. Sangiovanni Vincentelli, "Cyber-security for the Controller Area Network (CAN) communication protocol," in Proc. Conf. IASE Int. Conf. Cyber Security, 2012, pp. 344–350.
- [37] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the invehicle network in the connected car," in Proc. IEEE Intell. Veh., Symp., 2011, pp. 528–533.
- [38] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Creating a secure infrastructure for wireless diagnostics and software updates in vehicles," in Proc. Conf. Comput. Safety, Rel., Security, Tyne, UK., Newcastle upon Tyne, U.K., 2008, pp. 207–220.
- [39] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," in Proc. 19th Conf. USENIX Sec., Washington, DC, 2011, p. 6.
- [40] IEEE Standard for Local and Metropolitan Area Networks Part 16 Air Interface for Fixed and Mobile Broadband Wireless Access Systems, IEEE Std 802.16, 2009, IEEE Standard.
- [41] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in Proc. Conf. CRYPTO, 1993, pp. 232–249.
- [42] J. M. Alfred, P. C. van O, and A. V. Scott, Handbook of Applied Cryptography, Chapter-9-Hash Function. Boca Raton, FL, USA: CRC Press, 1997, pp. 359–368, no. 4.
- [43] S. You, M. Krage, and L. Jalics, "Overview of remote diagnosis and maintenance for automotive systems," in Proc. SAE World Congr., Detroit, MI, USA, 2005, pp. 1–8.
- [44] M. Shavit, A. Gryc, and R. Miucic, "Firmware Update Over The Air (FOTA) for automotive industry," in Proc. Conf. Asia Pacific Autom. Eng., Hollywood, CA, USA, 2007.
- [45] D. K. Nilsson and U. E. Larson, "Secure firmware updates over the air in intelligent vehicles," in Proc. IEEE Int. Conf. Commun. Workshop, Beijing, China, 2008, pp. 380–384.

- [46] H. Hilpert, L. Thoro, and M. Schumann, "Real-time data collection for product carbon footprints in transportation processes based on OBD2 and smartphones," in Proc. Conf. Syst. Sci., 2011, pp. 1–10.
- [47] J. Daemen and V. Rijmen, The Design of Rijndael. AES-the Advanced Encryption Standard. Berlin, Germany: Springer-Verlag, 2002.
- [48] K. Yasuda, "Multilane HMAC: Security beyond the birthday limit," in Proc. Conf. INDOCRYPT, 2007, pp. 18–32.
- [49] A. Hodjat and I. Verbauwhede, "Minimum area cost for a 30 to 70 Gbits/s AES processor," in Proc. IEEE. Comput. Soc. Annu. Symp VLSI, 2004, pp. 83–88.
- [50] S. Mangard, M. Aigner, and S. Dominikus, "A highly regular and scalable AES hardware architecture," IEEE Trans. Comput., vol. 52, no. 4, pp. 483–491, Apr. 2003.