SoK: Stealing Cars Since Remote Keyless Entry Introduction and How to Defend From It

Tommaso Bianchi
University of Padova
tommaso.bianchi@phd.unipd.it

Alessandro Brighente
University of Padova
alessandro.brighente@unipd.it

Mauro Conti
University of Padova
Delft University of Technology
mauro.conti@unipd.it

Edoardo Pavan
University of Padova
edoardo.pavan.3@studenti.unipd.it

Abstract

Remote Keyless Entry (RKE) systems have been the target of thieves since their introduction in automotive industry. Robberies targeting vehicles and their remote entry systems are booming again without a significant advancement from the industrial sector being able to protect against them. Researchers and attackers continuously play cat and mouse to implement new methodologies to exploit weaknesses and defense strategies for RKEs. In this fragment, different attacks and defenses have been discussed in research and industry without proper bridging. In this paper, we provide a Systematization Of Knowledge (SOK) on RKE and Passive Keyless Entry and Start (PKES), focusing on their history and current situation, ranging from legacy systems to modern web-based ones. We provide insight into vehicle manufacturers' technologies and attacks and defense mechanisms involving them. To the best of our knowledge, this is the first comprehensive SOK on RKE systems, and we address specific research questions to understand the evolution and security status of such systems. By identifying the weaknesses RKE still faces, we provide future directions for security researchers and companies to find viable solutions to address old attacks, such as Relay and RollJam, as well as new ones, like API vulnerabilities.

1 Introduction

The Remote Keyless Entry (RKE) and Passive Keyless Entry and Start (PKES) systems are access control mechanisms adopted in cars to open the doors and start the vehicle via a wireless channel. Specifically for the automotive industry, it dates back to 1982 when Renault used the patent deposited the year before for an infra-red remote controller [15]. Since its introduction, car manufacturers employed resources and research to improve their systems and provide more secure locks, for example, adding the immobilizer, an anti-theft system that requires authentication to start the engine [13]. In the last year, manufacturers have included the newest web and radio technologies in the automotive scenario, changing the paradigm of entering the vehicle. Relevant examples include PKES that do not require driver interaction, sophisticated keyless entries via smartphone applications [1, 5], or Near-Field Communication (NFC) cards acting as keys working on ultra-wideband signals to provide better security and comfort. However, these systems also increase the attack surface that thieves can leverage to enter, start, and steal the car [11]. Additionally, manufacturers' creation of custom closed-source devices and algorithms leads to vulnerabilities that can be discovered and used by malicious users. This could be solved without resorting to security by obscurity, having security researchers find vulnerabilities before attackers can, or that attackers may already use for real-world exploitation. Nonetheless, this field is still not getting the required attention by companies that see their cars stolen even nowadays [12]. In this paper, we provide the first fully comprehensive review of RKE and PKES technologies, attacks against them, and defenses in the automotive industry. To the best of our knowledge, no available contribution in the literature is providing a survey or SOK on this topic. We particularly devote our attention to the uncovered problems, analyzing how these systems evolved during the years, and answering the following research questions to provide an insight into the difficulties and problems to overcome to secure these systems.

> *Q1. Did the evolution of the RKE and PKES technologies increase their security?*

We explore the RKE history regarding technologies and tools to understand the impact of car hacking and if and how additional security measures were included. Secondly,

> *Q2. How did attack strategies evolve in time?*

We analyze the attacks found in the wild and in research papers to study whether the methodologies changed due to the new RKE systems or whether they are still vulnerable to *legacy* attacks. We particularly emphasize the attacker's needs and capabilities to open and start a car. We then focus on the

defense strategies.

> **Q3. Are currently existing defense strategies deployable and effective?**

We answer this question by checking if the defenses presented in the literature are deployable and usable by the car manufacturer for their systems or whether they are purely research-oriented. Lastly,

> **Q4. What do we need to develop an effective and secure remote entry system?**

To answer this question, we identify the open security issues that affect the RKE and PKES technologies comprehensively accounting for attacks to legacy systems and attacks to newer technologies. By answering this question, we provide future research directions in this field. Our work systematizes the different kinds of attacks discovered by researchers and used by thieves to steal cars, exploiting weaknesses in the RKE systems. We analyze attacks performed in the wild, thus that are authentic and feasible for thieves to access and start a vehicle in a real-world scenario In this way, we show the impact the RKE systems can have and the need for secure devices. The final objective is to answer the research questions, providing a helpful understanding of the history and current state of RKE systems, analyzing how the technology improved and how the weaknesses made it defenseless against attackers.

The contribution of this work can be summarized as follows:

- We extensively systematize and collect attacks and defenses on RKE systems, with more than 35 attacks since 2005 and 13 defenses specifically tailored for RKE proposed in the literature. At the time of writing, we are the first to provide a comprehensive review of the history and current state of RKE and PKES systems security research.

- We analyze the different technologies involved in these systems, such as the cryptographic functions and the physical layers used in RKE.

- We identify the weaknesses afflicting RKE and the evolution of attacks and defenses, pinpointing specific threats that persist until now and new attack surface, providing research directions for further exploration of this field. We specifically answer the research questions we posed, explaining how we reached such conclusions.

In the following, we describe the methodology in Section 2 and the background on RKE and PKES and their evolution in Section 3 and 4. In Section 5 and Section 6, we describe and analyze the attacks and the defenses in the vehicle remote and passive entry field. In Section 7, we answer the research questions, also trying to redirect the researchers interested in this sector to the new area of investigation (Section 8). Finally, we discuss the similar work in Section 9 and the conclusions in Section 10.

2 Methodology

The systematization study comprehends all the major attacks and defenses described in the four top conferences in cybersecurity, namely IEEE S&P, USENIX, NDSS, and CCS, with the addition of works with significant impact from the most respectful hacking and academic conferences, such as DEF CON and Black Hat. We selected works with a high practical impact, especially regarding the attacker side. Attacks targeting a fixed code radio signal are trivial, and we leave them out to focus only on the most interesting and recent aspect of RKE systems. Thus, our study starts with attacks against rolling codes, a security mechanism described in Section 3. The research on attacks specifically tailoring these technologies started in 2005, with the first security analysis of the cryptographic-enabled Radio Frequency Identification (RFID) device also used as RKE system. After that, researchers introduced different attacks and defenses in a cat and mouse play, adding new techniques and methods on both sides. In this sense, we describe these techniques associated with their corresponding technologies, analyzing the impact and the actuality of such methods.

3 Background

The Remote Keyless Entry (RKE) system patent dates back to 1981 from the inventor Paul Lipschutz [62]. Renault introduced the first RKE system in 1982 on board the Renault Fuego vehicle. From that moment, manufacturers adapted the car entry systems from the traditional physical key to the more technologically advanced key fob, integrating wireless commands to open or close the car's doors with a simple button press. This introduced an additional attack vector, as pointed out in different works after the rising use of this system [33, 82] and their first attacks. Also, two outstanding automotive researchers, Chris Valasek and Charlie Miller, especially pointed this out [85].

3.1 Remote Keyless Entry

Initially, the RKE system used an infra-red technology, as described in the patent by Lipschutz, with all the deriving difficulties and problems, such as the need to point the transmitter precisely towards the receiver [15, 31]. Now, they are based on radio frequency, with a short-range radio transmitter that communicates with the car in a range of 10-100 meters. The RKE system generally comprises a mechanical locking with the physical key blade, the remote entry system itself, and

an RFID-enabled immobilizer [13] to authorize and start the engine once inside the vehicle [71]. The key blade is included to insert and rotate it to start the engine as with a regular, physical key. Still, it is not needed to enter the vehicle (except in exceptional cases, such as dead battery or malfunctioning). The RKE system usually works using Amplitude Shift Keying (ASK) modulation for the physical wireless signal. Smaller groups of devices work on Frequency Shift Keying (FSK) modulation. The frequency depends on the regulation, standards, and regions, such as 315 MHz and 433.94 MHz for North America and Japan, where they follow the FCC 15 [68] (for RF devices) and the Association of Radio Industries and Businesses (ARIB) standards for radio frequencies such as the STD-T67 [70] and the STD-T93 [69]. Instead, in Europe, they operate at 868 MHz for Europe, following the CE mark directives for safety and regulations from ETSI EN 300 220 or ETSI EN 302 291 [50, 51]. The traditional RKE transmitter sends a command with a preamble, an identifier, the encrypted data field, and an integrity check field such as a Cyclic Redundancy Checks (CRC). To achieve security against possible thefts, the RKE system implements integrity protection mechanisms such as Message Authentication Code (MAC) and authentication. In general, the Original Equipment Manufacturer (OEM) follow the international ISO/SAE 21434 standard for security guidelines of these devices [40], where specific aspects and requirements for RKE systems dictate the design, implementation, and maintenance of a secure system. Indeed, the specific RF parameters are omitted in this international standard due to their regional dependence.

3.2 Passive Keyless Entry and Start

After RKE, the car manufacturer introduced the Passive Keyless Entry and Start (PKES). In its first implementation, it is a device with the ability to open the vehicle. Then, implemented in combination with the remote entry and the immobilizer. This technology does not require pressing a button, and the key fob is in continuous low-power listening mode to capture "wake-up" messages by the car's transceiver. The car broadcasts this message at a low frequency, generally 125 kHz, and wakes up the key fob to start the challenge-response procedure to authenticate and authorize the action. The two transceivers share the same secret key so that the key fob can correctly encrypt the challenge, usually composed by the encryption of a random number presented by the vehicle. Once the key is located inside the car as verified by Received Signal Strength Indication (RSSI) measurement for proximity, the vehicle also allows the ignition with the button for the engine to start. In PKES, we find the combination of Low-Frequency (LF) and Ultra-High-Frequency (UHF) technologies for the challenge-response mechanism, which could also be minimized to two messages in the case the vehicle also advertises its Car Identifier. Regarding guidelines for building these systems, the same regulations and standards discussed for RKE
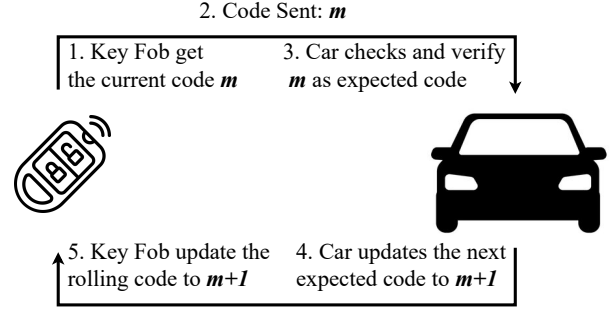

Figure 1: Basic example of Rolling Code usage, where the two parties updated the expected code at each iteration.

also apply to this technology.

3.3 Rolling Codes

In the beginning, the key fob used static codes during the communication. These static codes were prone to replay attacks due to the identical message transmitted with a press of the same button [26]. Thieves could easily steal cars by listening, recording a single button press, and retransmitting the signal. To avoid exposure to these attacks, manufacturers proposed using rolling codes. Rolling codes use a synchronized counter in the transmitter and receiver to generate one-time unique signals [63]. The transmitter includes the unique code in the message, and the receiver's side compares it against its local counter. If the values match, the receiver considers the signal valid, and both the transmitter and receiver increment their counter value. The car has a tolerance range to accept and re-synchronize the counter to foresee accidental button presses. Figure 1 represents a general and straightforward rolling code functionality. Nowadays, some rolling codes replace the incremental function with a more secure Pseudo-Random Number Generator (PRNG) with a shared secret seed between the receiver and transmitter [63]. These systems are thus more secure than static code, as they rely on cryptographic functions and usually closed-source schemes built internally by the manufacturers. However, they are prone to vulnerabilities, and, as we discuss later, attackers exploit them to gain access and take control of the vehicles.

4 RKE Implementations

In this section, we describe the evolution and implementations of the technologies for the RKE and PKES in more detail. We divide them into legacy technologies, based on rolling codes, and newer ones, using different physical channels and stacks, such as Bluetooth and web applications. Table 1 summarizes the systems, the technology they provide, and in which component we can find them. The complete and detailed description

of each system is out of the scope of this paper, and we refer to the bibliography for additional information. Yet, we provide the relevant specifications to understand the weaknesses exposing the RKE systems to attacks.

4.1 Legacy

The majority of the older techniques for RKE systems are based on cryptographically insecure schemes. Researchers and attackers identified their weaknesses over the years, significantly improving their security. Unfortunately, some are still present in key fobs nowadays, and attackers can leverage these systems for illicit car entry.

DST40. A Digital Signature Transponder (DST) is an RFID device supplying cryptographic functionalities for authentication. Texas Instruments designed it to provide security in vehicles via immobilizers, thus requiring authentication before ignition [30]. It is a passive device; therefore, it receives its power via electromagnetic induction. This device's peculiarity is that it uses a 40-bit cryptographic key, programmable via Radio-Frequency (RF) commands. The DST emits an identifier of 24 bits and authenticates with a challenge-response protocol, with a challenge of 40 bits and a truncated 24-bit response. The security of this device depends entirely on the secrecy of the key. Due to the low number of bits used, the vulnerabilities found in this system forced companies to adapt the RKE systems, increasing the number of bits (see DST80) or with new ciphers.

KeeLoq. KeeLoq is a block cipher used in RKE systems and immobilizer. It consists of a 32-bit block size and a 64-bit key. KeeLoq uses two registers: key register and state register. It can be viewed as a Non-Linear Feedback Shift Register (NLFSR) that depends on the above two registers. At each iteration, the registers are shifted to the right, and an XOR function computes the new bit; after 528 cycles, the ciphertext is in the state register [38]. To authenticate the transmitter, KeeLoq provides a challenge-response protocol in rolling code applications with two keys: the device key, shared and unique to each pair of transmitter and receiver, and the manufacturer key used to derive the device keys.

Hitag2. It is a stream cipher used in immobilizers from different car manufacturers. It is a proprietary cipher, but researchers reversed it in 2007 [91]. Hitag2 implements a 48-bit key as the structure of the internal length of the scheme [99]. The chips contain eight pages of 32 bits for 256 bits in total. It can work in distinct modes depending on the objective: read-only, writable (*Password mode*), and *Crypto mode* for additional security. The *Crypto mode* is the one implemented on vehicles' key fobs. In this mode, the transponders share a secret 48-bit key, with a unique Initilization Vector (IV) generated for each transmission to avoid replay attacks. Together

with the serial number of the tag transponder, the IV and the key initialize the cipher that produces a keystream, with the first 32 bits used for authentication and the other 16 bits for encryption.

Megamos. Car manufacturers used Megamos Crypto in the immobilizer. Introduced by EM Microelectronic-Marin SA, it consists of a 96-bit secret on a proprietary cipher, with a 32-bit code needed to write in memory. The authentication proceeds with the car sending a random nonce to the fob with a car authenticator (identifier), and the key fob responds with its authenticator [86]. The authors in [88] reversed the cryptographic scheme, identifying a stream cipher with five main components working as a PRNG.

DST80. After the problems found in DST40, in 2012 Texas Instruments presented the newer DST80 [52]. It uses an 80-bit authentication key stored in two halves and can support fast or mutual authentication [95]. The authentication protocol follows one of its predecessors with a challenge-response scheme but also includes a block check and a signature.

In legacy systems, the implementation of weak cryptographic measures dictated the development of new cryptographic tools to overcome the previous problems. The RKE systems, independently from the ciphers used, suffer from the physical layer attacks such as relay, jamming, and replay, as we discuss in later sections. The reason is that these attacks work directly at a signal level without breaking or interfering with the encryption mechanisms. The impossibility of overcoming these vulnerabilities led to adopting new technologies that mitigate the problem, such as Bluetooth and Ultra Wideband (UWB) communication.

4.2 New Technologies

With the advent of new technologies, car manufacturers found opportunities to introduce them in their products. Different RKE nowadays implement the use of NFC with cards or Bluetooth through a smartphone application. As with any other technology, the comfort they bring comes with the price of decreased security if not properly and carefully implemented. Nonetheless, these systems promise to reduce the risk of attacks and defend against physical layer attacks that, as previously mentioned, are harder to mitigate due to their nature (relaying, replaying, and jamming).

NFC. It is a set of protocols to enable communication between two devices in a short-range scenario. Different standards extend the RFID [14]. Tesla Motors introduced this car access method on the Tesla Model 3 [81]. To open the car, the driver needs to tap the NFC card against the card reader on the door pillar on the driver's side. After that, the driver has

Table 1: Vehicle remote entry technologies and evolution. The first five rows represent rolling code schemes, while after that, we saw the implementation of other protocol stacks, such as NFC and web services for vehicle connection to the internet. The acronyms are RKE - Remote Keyless Entry, PKES - Passive Keyless Entry and System, IMM - Immobilizer. The symbol ● indicates in which component the system is mounted.

System	Technology	Component		
		RKE	PKES	IMM
DST40	40-bit proprietary challenge-response protocol working over RFID from Texas Instruments			●
KeeLoq	Proprietary Non-Linear Feedback Register Rolling-Code application	●		●
Hitag2	Proprietary stream cipher working on a 48-bit key from NPX semiconductor			●
Megamos	96-bit secret on a proprietary stream cipher			●
DST80	Texas Instruments 80-bit DST improvement with signature			●
NFC-based	Set of protocols for communication in short distance to open the vehicle		●	●
BLE-based	Wireless Personal Area Network to connect to the vehicle		●	
UWB-based	Radio technology for low energy signals and higher data rates for vehicle-RKE communication		●	●
API-based	Handlers for different actions requested by applications to communicate with the vehicle through the internet connection	●	●	
Third-Party Applications	Applications to provide better control or services with car manufacturers	●	●	

two minutes to start the car, or it must be re-authenticated by placing the card on the internal reader.

Bluetooth Low Energy (BLE). BLE is a well-known wireless personal area network radio interface technology. It is designed for energy-constrained devices and establishes a client-server (phone/car) connection. Tesla introduced it as a vehicle key via its application [81].

Ultra Wideband (UWB). It is a radio technology for short-range communications using a wide bandwidth to send signals with very low energy. It uses different channels splitting the bandwidth into smaller chunks to favor higher data rates [9]. In 2021, BMW announced and later implemented UWB in its digital keys with increased security and comfort [17]. In their statement, they promise security against the infamous relay attack, which we discuss in Section 5.

As we describe in the next section, the use of these technologies does not fully mitigate the possibility of attacks to RKE and PKES systems. The introduction of web and smartphone applications can not only increase the usability and comfort of the users but also help in defending against theft and attacks by sending messages through these channels.

4.3 Advent of the Web

In recent years, the automotive sector has seen the opening to the web as a tool for collecting vehicle data and diagnostics. Nowadays, the web is also used to provide new smart features to cars and their owners. Opening a car and starting the engine or opening the heating is possible through the touch of a button on a smartphone. This introduces a new attack surface that largely increases the possibility of errors for developers and the exploitation by attackers, as in the everyday web security field [19].

Application Programming Interface (API). The use of this web application system requires the implementation of APIs to handle the different actions [2]. These are not limited to opening or closing the doors but are also used by manufacturers to query the car for diagnostic data. Different car manufacturers have closed APIs, but researchers are working on reversing them as it happens with Tesla [8] or Kia [21].

Third Party Apps. To provide better control of cars, different manufacturers allow the integration of third-party applications, also integrating additional APIs. The drivers are turning towards these providers because they offer better features at a lower price, sometimes also coming with transparency on the data usage [7]. Also, in this case, introducing third parties in the system increases the attack surface available for malicious users [67, 76].

Even if these systems can help prevent attacks and increase the complexity of possible exploitations, the web introduces all the risks associated with it, such as the normal web exploitation vectors, as we describe in the next section.

5 How They Steal Your Car: Attack Strategies

In this section, we describe the macro-area of attacks against RKE systems and the exploits implemented in real-world scenarios during the years, showing the similarity between the first attacks and the upcoming ones in these last few years. Table 2 contains all the attacks divided by type and in chronological order, indicating the target of the exploit. As we can see, cryptographic attacks highly focus on retrieving the secret key from the devices. We left out lock picking from the attacks due to the physical and not RKE related nature.

The different areas consist of the kind of attack and means to carry it. Specifically, we have cryptographic attacks and different wireless signal methods to intercept and break the RKE systems. Some attacks combine the different classes to exploit weaknesses in a cipher, retrieve the key craft authenticated packets, or perform other attacks subsequently. Section 5.1 describes the various cryptographic attacks presented in the literature. In Section 5.2 and 5.3, we present the attacks based on radio technologies such as jamming and replay, while in Section 5.4, we show how new technologies employed in these systems still present weaknesses and introduce an exploitable point leveraged by attackers. Finally, in Section 5.5, we describe the weaknesses of introducing web technologies into the automotive industry related to the remote keyless entry.

5.1 Cryptanalytic Attacks

This category includes all the attacks that target the cryptographic functions implemented inside RKE, PKES, or immobilizer. Generally, these attacks require access and recording of some messages between the car and keyfob and reverse engineering the algorithm, ultimately allowing the recovery of the key and cloning the keyfob. Additionally, they affect all the companies and brands using the same type of cryptographic tools inside their keyfobs.

Exhaustive search. The most straightforward approach for the attacker is to search through all the possibilities. Depending on the search space (e.g., key size), it may require significant time but eventually converges to a solution. The search space can also be decreased by exploiting weak ciphers and keys. This method allows the attacker to find the key for the RKE system. The first attack in this category is the cracking of DST40 by [30]. The authors reversed the protocol and needed only two challenge-response pairs to recover the keys.

Over the years, different exhaustive search attacks allowed hackers to steal the RKE and PKES keys.

After [30], researchers broke the (in-)famous Hitag2 in 2011 [99] and [28]. The first attack details a new method for breaking the stream cipher with only two sniffed messages and significantly less time than the available algebraic attack: 2 hours instead of 45, thanks to the hardware implementation on COPACOBANA platform. In [28], the authors performed a black-box analysis. They identified a weakness in the initialization vector that allows an attacker to find the key in minutes with access to a cluster to perform an optimized brute force search.

Even the other ciphers, such as Megamos and DST80 were not secure, as Verdult et al. [88] and Wouters et al. [93] showed in their works. The first work presents the inner functionalities of Megamos Crypto, showing its weaknesses and how to exploit them to recover the 96-bit key with a computational complexity of 2^{56} cipher ticks (or 2^{49} encryptions). They target various car makers and models, finding they used weak keys (only ten over 96 bits were ones) that allowed for a partial key-update attack with additional optimization. In 2019, Wouters et al. reversed the DST80 cipher used in the Tesla Model S vehicles PKES, revealing only 40 bits system, lack of mutual authentication, and other memory vulnerabilities [93]. These vulnerabilities allowed the attackers to clone the key fob quickly from a challenge-response round with a Man-In-The-Middle (MITM) attack, employing a time-memory trade-off technique to reduce the computation time to recover the key.

Guess-and-Determine (GD). Guess-and-Determine (GD) is a technique used in cryptanalysis to recover unknown variables in a system. It consists of guessing a subset of the variables in order to deduce the remaining values and their relationship [89]. This is particularly useful when the cipher does not use the whole internal state to compute the keystream (stream ciphers). The attacker can initially guess only a partial internal cipher state and evaluate the output, drastically reducing the search time compared to the exhaustive methodology. The first work using this method against RKE systems attacks the KeeLoq and its self-similar key schedule to guess a portion of the key using the sliding technique to generate pairs of input and output [29]. Ultimately, the author recovered the entire key by deducing linear relationships with the key bits with a complexity of $2^{50.6}$ (with a more involved attack with 2^{37} complexity) with the requirement of 2^{32} known plaintext-ciphertext pairs. Researchers also used the GD technique to break the Hitag2 ciphers. Vergesten et al. improved the GD attack on Hitag2 key recovery through different optimizations [89]. The authors claim an improvement of over 500 times with respect to the previous fast Hitag2 attack [28]. These attacks allow the recovery of the keys and, ultimately, from the reverse engineering of a single internal state, clone the keyfob.

Table 2: The attacks targeting RKE and PKES systems grouped by the attack class. The acronyms for the attack targets and goals are as follows: RKE: Remote Keyless Entry, PKES: Passive Keyless Entry and Start, IMM: Immobilizer, AC = Action on Car (open the doors or start the car), SK = Secret Key retrieval, CK = Clone the Key fob. The ● symbol means an attack against a target and following a specific goal. In contrast, the ◑ symbol indicates if it is related to that domain due to a side effect (e.g., the attack targets the RKE system but can also be used to start the car through the immobilizer bypass).

Attack Class		Attack	Target			Goal		
			RKE	PKES	IMM	AC	SK	CK
Cryptographic	Exhaustive Search	Analysis of DST40 [30]	◑		●		●	◑
		Hitag2 hardware optmization [99]			●		●	
		Megamos Crypto [86, 88]			●		●	
		Hitag2 optimized attack [28]			●		●	
		Analysis of DST80 [93]		●			●	●
	GD	KeeLoq Cryptanalysis [29]	●		●		●	
		Hitag2 optimized GD [89]			●		●	
	Slide Attack	KeeLoq Algebraic and Slide attack [34]	◑		●		●	
		Practical attack on KeeLoq [49]	●		●		●	
	Algebraic Attack	KeeLoq Algebraic and Slide attack [34]		●			●	
		Hitag2 practical algebraic attack [35]			●		●	
	Correlation Attack	Hitag2 dependencies between sessions [87]			●		●	
		Insecurity of Hitag2 RKE systems [42]	●		◑	◑	●	●
	Power Analysis	KeeLoq Code Hopping [38]	●		●		◑	●
		Extarcting KeeLoq keys [58]	●		●		●	
		Dismantling the DST80 immbolbilizer [94]		●			●	
Relay Attack		Relay on PKES systems [41]	●	●	●	●		
Jamming and Replay Attack		RollJam [78]	●	●	●	●		
		RollBack [36, 61]	●	●	●	●		
		RollingPwn [18]	●	●		●		
		RollJam with known noise source [37]	●	●	●	●		
		RollJam revisited [79]	●	●	●	●		
Bluetooth and NFC		TESLA Model 3 NFC Relay [24]		●		●		
		Tesla Model X PKES compromising [92]		●				●
		Ghost Peak: UWB distance reduction [60]	●	●		●		
		BLE Phone-as-a-key Relay [59]		●		●		
		Tesla Model 3 RKE compormising [96]	●	●				●
Web Services		Remote Started admin API [55]			●	●		
		Exploitation of Honda Connected App [32]	●			●		
		SiriusMX API [66]	●			●		
		TeslaMate API [6]	●			●		
		Tesla Logging Web Service [77]	●			●		
		Kia Service API [22]	●			●		

Slide attack. This cryptanalysis technique aims to break a cipher in multiple rounds identified in identical function representations [47]. A slide attack deals with ciphers with a high number of rounds, rendering complexity-based security ineffective. In the literature, two works from 2008 focus on slide attacks against KeeLoq. The first work, proposed by Courtois et al. [34], combines the algebraic and slide attacks to noticeably simplify the key recovery by guessing 16 bits, corresponding to the last 16 rounds and thus reducing the total number from 528 to 512 with a total complexity of 2^{53} KeeLoq encryptions. The drawback is the requirement of 2^{16} known plaintexts. In the second paper, Indesteege et al. [49] reduced the complexity to $2^{44.5}$ KeeLoq encryptions with 2^{16} chosen plaintexts (same requirement of the previous attack) thanks to a new meet-in-the-middle approach. They fully implemented the attack, which recovered the master key in less than five minutes and replicated the full device.

Algebraic attack. It expresses the cipher as algebraic equations, replacing the known data in the system and trying to search for the key. The technique is highly successful against ciphers using linear operations, while systems combining non-linear functions make this method harder to utilize. In [34] and [35], Courtois et al. proposed two algebraic attacks first against KeeLoq, described before in the Slide attack paragraph, and against Hitag2. In both works, they leveraged SAT solvers to represent and solve the system of multivariate equations, guessing some variables and examining the consequences. In [35], they focused on the challenge-response Crypto mode of Hitag2, with a Known IV attack to make it practical. It requires data from 4 transactions, guessing 14 bits of the key, and combining the equations for the four known IVs. It requires around two days for the full 48-bit key, but it is fully automated and can work against Hitag2 with slight modifications.

Correlation attack. A correlation attack is used against stream ciphers that combine different Linear Feedback Shift Registers (LFSRs), using their output as boolean functions. This attack exploits the correlation arising from statistical weaknesses. The two attacks in this category represent some of the main works against RKE systems exploiting cryptographic weaknesses in Hitag2.

"Gone in 360 Seconds", by Verdult et al. [87], uses the lack of PRNG and redundancy as an arbitrary length keystream oracle. The authors also observed a one-bit leak in the secret key for every four authentications and 16-bit persistent information in the secret key over multiple sessions. They presented two attacks: the first one uses the first vulnerability and uses a keystream shifting attack, while the second one is against the LFSR and is more general. Their evaluation of 20 different cars found that the LFSR seed was based on time, introducing weak and predictable (or even default) passwords and low entropy keys. With these vulnerabilities, they were able to use correlation to predict possible keys and perform a dictionary attack due to the low entropy of the keys.

The second main work by Garcia et al. [42] analyzed the Volkswagen group, finding that they used only a few global master keys. In this way, they could clone remote controllers by eavesdropping only one signal. Against Hitag2, they described a novel correlation attack, called *fast-correlation attack*, recovering the key with only 4 to 8 signals in one minute of computation. To do so, they make guesses on the counter window, which initializes the cipher with a 28-bit counter. They found that only 10 bits were used over the air by reverse engineering; therefore, the attacker needs to guess the remaining 18 bits. After that, the attacker clones the key fob and can access the vehicle for further exploitation.

Power Analysis. Power analysis consists of a side-channel attack aiming to extract the secret key by analyzing the power consumption of the hardware during cryptographic operations. Power analysis against RKE systems focused specifically on KeeLoq in 2008 and 2009 [38, 58], with a recent work against DST80 [94]. Eisenbarht et al. [38] demonstrated that ten power traces are enough to clone a remote controller and extract the manufacturer key with differential power analysis. Once the attacker knows the manufacturer key and key derivation algorithm, it can also perform power analysis on two hopping code messages eavesdropped from the remote. This is possible because the KeeLoq remotes analyzed do not use any seed for key derivation. In [58], the authors use simple power analysis to extract the key, drastically reducing the time required (seconds) for the operation with respect to the previous attack. In this case, only one measurement is enough to extract the 64-bit master key. Concerning power analysis in this environment, there is a more than ten-year gap until Wouters et al. published an attack against DST80 in 2020 [94]. They exposed significant flaws in key diversification schemes used by major car manufacturers like Toyota, Kia, and Hyundai, revealing extremely low entropy in the generated keys. In this paper, the authors used voltage glitching to extract the firmware and side-channel attacks to recover the cryptographic key. The same authors in [93], unveiled the incorrect use of DST80 as identical to the DST40, thus inheriting the older vulnerabilities and weaknesses.

As we described, some cryptographic attacks combine multiple techniques to reach the goal of extracting the secret keys and cloning the key fob. Nowadays, these attacks are less applicable due to the change in the RKE and PKES systems. Nonetheless, security vulnerabilities are always a threat, especially in cryptographic closed-source functions that lack proper testing.

5.2 Relay Attacks

A relay attack is a MITM combined with a replay attack. Specifically in RKE scenario, the attacker manipulates the
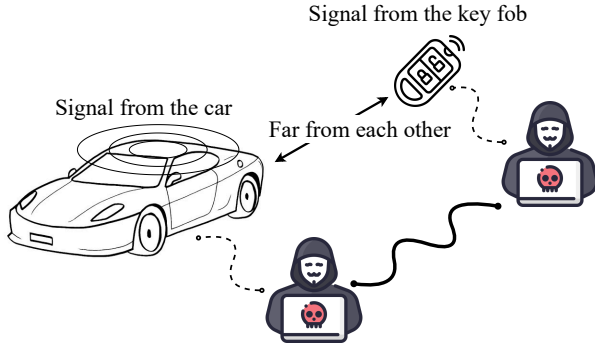
Figure 2: Relay attack representation where the two bad actors intercept the signals from the vehicle and the key fob, tricking them into thinking they are in close range.

communication between the transceiver on board the vehicle and the key fob, intercepting and forwarding the message in an intermediary channel to cover the distance separating the two devices [53]. In this way, the car transceiver thinks to be in the area of the key fob and to communicate with it. The same happens in the opposite direction, with the key fob believing being close to the car range. In Figure 2, we show the steps for the attackers (usually two partners) to relay the signal and steal a car. This attack targets all the legacy systems independently of the model and car manufacturer.

Francillon et al., back in 2011, proposed the relay attack against vehicles and PKES systems [41]. They built the attack in the experimental scenario with 10 cars measuring the distance reachable to open the vehicle, relaying both the LF and UHF signals of the PKES, also with amplification. They found that without amplification, they could reach up to 2 meters from the car, while with an amplified signal, this range extended up to 8 meters. On the opposite, the distance from the key fob, due to the use of higher frequencies, could be up to 60 meters. The authors note that the main reason for the success of this attack is the verification of communication with the correct key, but not that the correct key is in proximity. The communication condition is (wrongly) assumed to be verified if the two devices communicate, thus deeming only key verification necessary. As this attack shows, this wrong assumption makes the exploitation possible, and the PKES systems are still vulnerable due to the same weakness [44, 83].

5.3 Jamming and Replay

The Jamming and Replay attack, also called RollJam, was first introduced in 2015 by the security researcher Samy Kamkar [78]. The attack requires very low-budget hardware as Software Defined Radio (SDR) and targets the RKE and ignition of cars using rolling codes. It consists of recording and blocking the radio signal from the key fob when the driver

tries to unlock the doors. The driver will try again to unlock the vehicle. Still, the attacker will execute the jamming and recording against the second signal while replaying the first recorder message to let the driver think the unlock worked the second time. Now, the attacker has a second, valid code to unlock the car, and the driver will lock it the next time. In Figure 3, we represent the attack steps. Starting from this attack, different researchers improved the procedure or proposed alternative approaches. Also, many people tried it against various vehicle brands and models, confirming and proving the exploitability of this attack in the wild [16, 27, 48, 79, 84]. Especially these last works present simple solutions to perform the RollJam attack and analyze and test RKE systems automatically [79].

The first work targeting the vehicle opening mechanism is RollingPwn [18]. The ten most popular Honda vehicles from 2012 to 2022 are affected by this vulnerability of the rolling code mechanism. The Honda's weakness consists of accepting codes from a rolling code from the previous cycle after resynchronizing the counter. The authors published the attack on a webpage after Honda Motors stated that this replay method would not work against their key fobs implementing rolling codes.

The second attack using the Jamming and Replay paradigm is RollBack by Levente et al. [36, 61]. They presented a setup similar to RollJam, but they only recorded the second unlock signal instead of jamming it. After that, the owner can use the car as many times as it wants. The attacker can replay the two consecutive packets and unlock the car thanks to a resynchronization to a previous state with the first signal. The authors confirmed the vulnerability of Kia and Mazda vehicles.

The latest work improves the RollJam attack using a known noise source, rebutting the requirement of specific knowledge of the attack surface and SDR parameters for the original attack [37]. Using a known noise signal for jamming introduces significant improvements in the attack success rate, in contrast to the additive white Gaussian noise used in the original work.

5.4 Attacks Against New Technologies

In recent years, multiple car brands have redesigned the RKE and PKES systems to new technologies such as Bluetooth, NFC, and UWB. Utilizing these communication technologies made stealing a vehicle harder but not impossible. In fact, various researchers found weaknesses inherited by the protocol stack or a broken implementation of the communication mechanism.

Starting in 2020, the hacker named Kevin2600 and its Chaos-Security-Lab presented a relay attack against NFC opening used by Tesla [24]. They analyze the internals of the key fob and the NFC Tag (in this case, a Java smart card). They use an Android application called NFC-Gate to perform
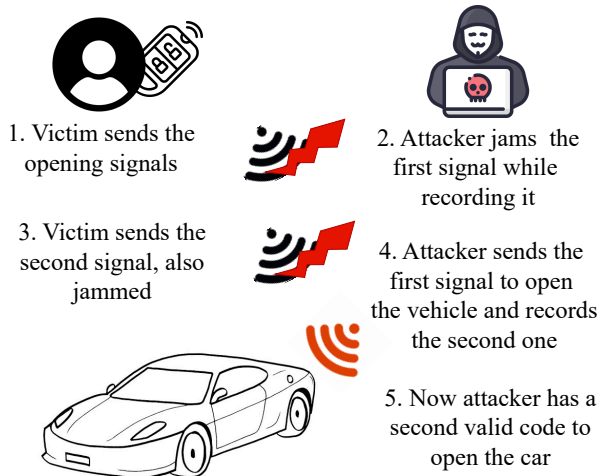
Figure 3: Rolljam attack steps representation, in which an attacker jams and sniffs the two signals from the victim while sending the first capture during the second jamming.

a MITM attack, reversing the NFC communication and actuating a relay attack against the Tesla with a relay transmission over WiFi. They reported the findings to Tesla, who answered without much attention and suggested using the additional security called Pin2Drive (inserting a pin inside the vehicle to start the car). They also checked for the pin, which had only four digits, without any brute-force protection. Also, in this case, they could still access the car.

After that, in 2022, researchers in NCC Group found a relay attack on the BLE link layer [59]. It was possible to add latency within the normal GATT response timing variation to make relaying of the encrypted link layer possible. In addition, this attack could bypass the relay mitigations and bounds accepted by the Tesla Model 3 PKES. Always against Tesla, a year later, Xie et al. reverse-engineered and exploited the Phone Key feature through a MITM attack on the Bluetooth channel [39, 96]. Additionally, they found a weakness in the Key Card pairing protocol, allowing them to connect a programmable Java card. Combining the several flaws explained in their paper, the authors could trick the vehicle into believing that the phone used by the attacker was authenticated and registered, thus allowing the attacker to enter and start the car without any awareness by the actual owner.

A work not strictly related to the channel communications presented before, even if passing over BLE, targets the PKES and Body Control Module (BCM) of the Tesla Model X to unlock and start the vehicle [92]. Two vulnerabilities allowed the researchers to compromise the system: the firmware on the key fob did not properly verify the image's authenticity through the BLE interface, and the pairing protocol never sent the certificates to verify the key fob's authenticity to the car. Combining the two vulnerabilities, they were able to unlock

and start a Tesla in a few minutes, assuming access to the Secure Element in the key fob. The researchers built a portable device that could carry out the attack, using modified Tesla components to wake up a target key fob, install malicious firmware, and pair a rogue key fob to the vehicle.

Concerning UWB technology, car manufacturers started to include it in the new RKE systems in the last few years, as introduced in Section 3. Since the introduction started around 2021, researchers already found weaknesses even after the promise of UWB being secure against relay attacks. Leu et al. presented the first over-the-air attack on the UWB measurement system [60]. The authors could reduce the perceived distance in the high-rate physical layer settings, called High Rate PHY (HRP). In this attack method, the power of the injected packet is selectively varied per packet field to avoid being perceived as a new packet or as jamming. The researchers refer to this attack as *selective overshadowing*, in which the attack signal is synchronized with the legitimate signal. However, the attacker does not need to know a specific packet field for security applications. In their experiments, the authors reduced the measured distances from 12 to 0 meters with a success rate of 4%, sufficient to deceive ranging systems that rely on single HRP measurements. This attack is particularly important for the possible implications in the RKE scenario. During the last year, Wired reported the criticalities of UWB and their implementations in the automotive industry: Tesla vehicle could still be stolen by the old-fashioned relay attack against Bluetooth due to the absence of using UWB for distance checking [4, 45].

5.5 Web Service Exploitation

The automotive environment is more and more connected to the web realm. A multitude of services are available for connected cars, including the RKE remotely managed, for example, through an application on a smartphone. Different platforms and third-party applications can also interact with vehicles, leaving space for common attacks from the web space. First, APIs interacting with the cars can introduce attackers into the system, as shown in the Jmaxxz work presented in 2019 [55]. Jmaxxz found a remote starter on the web that uses an application as a remote. The author found the firmware and where it needed access to the Internet, revealing an API key with default user and password and a SQL injection attack to become the administrator. From there, Jmaxxz could start the car with another SQL injection vulnerability. A multitude of works targeted the API as the remote exploitation of Honda cars in 2022 [32] or the SiriusXM connected vehicle service vulnerability that exposed cars from Honda, Nissan, Infiniti, and Acura [65, 66]. In both cases, the researchers found vulnerabilities in the applications and API that allowed them to bypass account security and execute remote commands, such as unlocking the cars. In 2023, a security researcher was able to access Tesla cars all over the

world thanks to a vulnerability in the APIs of a third-party application (TeslaMate) used to track the vehicle's movements and perform some actions, including unlocking the doors [6]. Other vulnerabilities allowed access to the cars through web applications for logging or improper account and request validation [22, 77]. Different other vulnerabilities can also give access to private information and actions to malicious users, and different brands are involved, also from major manufacturers such as Rolls Royce and Porsche [20]. This highlights how the increasing interconnection between automotive and the web is drastically enlarging the attack surface, with targets that can differ from unlocking the vehicle's doors.

6   How Researchers Defend From Thieves

This section presents the research and possible defensive techniques available for RKE and PKES schemes. The solutions presented differ in the method and the technology adopted, ranging from distance bonding protocol to a newer proposal based on a quantum key distribution protocol to be safe in the post-quantum era. In Table 3, we overview the researchers' defense proposals and the attacks they mitigate. We will not discuss, if not briefly at the end of the section, the immediate-term and mid-term solutions found in the attack papers due to their inadequate usability for the RKE, such as the battery removal, shielding the key fob (thus a viable option), or kill-switch for the key fob functionalities. We focus only on the long-term and new paradigm proposals to defend the RKE system, dividing them based on the mitigation against Replay/RollJam or Relay attacks, except for one work that aims at protecting against power analysis. Due to the broader scope and general mitigation and defenses for APIs and web services, we still do not see significant research on web security explicitly related to automotive.

In general, academic research to defend the RKE systems in automotive is recent and started around 2017. The sole work preceding this time is coping with the significant threat of power analysis, which was published in 2009 [64]. The authors proposed a RKE with PRNG and dynamic re-keying strategy to ensure a unique session key, thwarting side-channel attacks that rely on fixed keys. To work, the transmitter and the receiver synchronize the PRNGs and initialize with random input and output securely transmitted. This remote entry is resistant to side-channel analysis and ensures privacy against profiling and the manufacturer, which can not exploit the system with a global key.

6.1   Replay and RollJam Defenses

The replay attack has been present since the introduction of the first RKE systems due to the ease of application, especially on fixed codes and in the absence of timestamps. In addition, as demonstrated by [78], even rolling codes do not secure entirely against them. In this case, the attacker needs to

be in the range of the real remote system and steal the signals while jamming it when the car's owner closes or opens it. The requirements are more complicated to achieve than in a relay attack, but it is still feasible and explored in the wild. The defender side needs to get a more complex authentication mechanism without adding a noticeable delay by the user. The mechanism could add cryptographic operations or more steps in the authentication, which means a trade-off between security and usability. In 2017, Glocker et al. tried to end this threat by introducing a symmetric key encryption scheme in the RKE [43]. The key fob and the onboard computer authenticate themselves using 2000 randomly generated numbers allocated in memory. Both parties then compare the received messages by using their memory locations. The protocol secures RKE against scan attacks, playback attacks, two-thief attacks, and jamming with a specific implementation built on the car. A year later, in 2018, researchers briefly analyzed the security of vehicles RKE systems and proposed a defense mechanism involving a Secret Unknown Cipher (SUC) with a tamper-resistant physical identity module used for key derivation and encryption operations [75]. The security comes from using the unclonable security module and builds its system over vulnerabilities found in [43]. They opted for pseudo-identities for the vehicle and encrypted challenge-response messages. The authors also implemented the proposed system using Raspberry Pi 3 and piVirtualWire library to evaluate its practicality. They found that the computational time of the key fob was acceptable for real-world use. The timestamp-based defense mechanism proposed in [46] deals directly against the replay attack, enhancing the existing rolling code RKE systems. The proposal adds a timestamp and a second-factor authentication to a randomly generated rolling code, all encrypted with Advanced Encryption Standard (AES) with a 16-byte key. The receiver determines the validity of the received signal, checking if the timestamp is in a window of 100 seconds.

Lastly, Parameswarath et al. have proposed three different mechanisms to defend specifically against the RollJam attack. In the first paper, they presented a Physical Unclonable Function (PUF)-based lightweight mutual authentication [74]. Using PUFs, the system makes the prediction or replication of the challenge-response messages impractical. Theoretically, using these primitives makes the protocol faster and more secure than previous proposals, but the authors only formally proved it. Instead, the second work uses hashing and asymmetric cryptography, but it requires a setup phase to transmit the public key [73]. In the authentication phase, the key fob generates a random number, combines it with the current date and time, and calculates the hash value, then transmits it with a signature. Also, only informal security analyses and simulations are present in this paper. Lastly, Parameswarath et al. proposed a quantum-safe authentication protocol with Quantum Key Distribution (QKD) [72]. It aims to build a secure symmetric key against quantum attacks. The advantage of

Table 3: Defenses presented in this work. The acronyms for the target mean C = Crypto, R = Relay, JR = Jamming and Replay, NT = New Technologies, WA = Web Applications. The acronyms for the devices are as before. RKE stands for Remote Keyless Entry, PKSE for Passive Keyless Entry and Start, and IMM for Immobilizer. The ● symbol indicates which attack the defense wants to mitigate or remediate and the devices it uses. *N/A* indicates the paper does not make values available.

Defense	Cost (ms)		Target					Device		
	Key	Car	C	R	JR	NT	WA	RKE	PKSE	IMM
RKE power analysis defense [64]	N/A	N/A	●					●		
RKE Symmetric-Key Cyrptography [43]	4	4			●			●	●	
General RKE strengthening [75]	13	N/A			●			●	●	
Timestamp-based defense [46]	N/A	N/A			●			●		
PUF-based RKE mutual authentication [74]	0.103	0.097			●			●		
Authentication tailoring RollJam [73]	10	10			●			●		
Quantum safe RKE Authentication [72]	N/A	N/A			●			●		
Distance bonding based RKE [41]	N/A	N/A		●				●		
UWB with Pulse Recording [80]	N/A	N/A		●		●		●	●	
Context-Based Secure RKE [90]	N/A	N/A		●				●		
Time-based Countermeasure on PKES [97]	N/A	N/A		●					●	
Machine Learning relay protection [25]	N/A	N/A		●				●		
HODOR fingerprinting for RKE [56,57]	<500	<500		●				●	●	

this system is the possibility of understanding the presence of an eavesdropper.

6.2 Relay Protection

The relay attack, introduced in 2011 by [41], is still a threat nowadays, with cars stolen with the same technique described in Section 5. The relay attack is easy to perform and does not require very costly hardware, and due to this reason, more attackers adopt it to steal cars. On the opposite, defending against it is challenging due to the physical nature of the attack and the requirement to use different hardware and physical layers to cope with it. Also, the time frame in which it is possible to carry the relay attack is very short, leading to a more difficult detection. In [41], the authors proposed the first possible high-level solution based on distance bounding protocols. This method requires accurate distance measurements and multilateration with multiple devices inside the car while trusting the key fob. The car performs a secure distance bounding protocol and unlocks the doors if the key fob is in a specific range. Singh et al. proposed the use of UWB with *pulse reordering* in 2019 to provide resilience to physical-layer attacks with high performance [80]. It uses random reorders of UWB pulses associated with a set of consecutive bits using a permutation that is a shared secret between the communicating devices. Additionally, it applies a cryptographic XOR operation to the polarity of pulses with a pseudo-random sequence, making the pulse sequence appear random to an attacker. This system is compatible with pre-existing UWB technologies and standards to provide better interoperability and employability. The authors provided experimental evaluations to demonstrate that UWB with pulse reordering achieves a low bit error rate comparable to standard implementations, proving that security enhancements do not degrade communication performance.

Researchers presented two other works in the same year. The first paper introduced a context-based RKE system to prevent relay attacks based on BLE communication between the key and the vehicle [90]. Collecting data from the environment such as signal strength indicator, messages round-trip time, Global Positioning System (GPS) coordinates on the key fob, and a radio environment with Wi-Fi, this method determines the key fob's proximity to the vehicle. The implementation uses a smartphone as a key fob and detects anomalies (with a machine learning algorithm such as Decision Tree) while preventing relay attacks. Instead, the second paper examines time-based countermeasures for relay attacks against PKES systems [97]. They compared two time-based measurements, Time of Arrival (TOA) and Difference Time of Arrival (DTOA), in distance-bounding protocols. The authors presented three different TOA-based estimation methods after concluding that the DTOA is not suitable for distance-bounding applications due to its higher uncertainty. Simulations are available to support their protocols for estimation accuracy. The three methods provide a trade-off between accuracy and computational load (accompanied by energy consumption). The relay protection can also rely on machine learning algorithms, as demonstrated by Ahmad et al. [25]. Their solution detects relay attacks using machine learning on key fob signals (time, location, signal strength). It verifies the driver via Long Short-Term Memory (LSTM) neural networks analyzing driving behavior, such as acceleration and braking. It prevents unauthorized access and driving with 99.8% and 81% accuracy. The algorithm is implemented on

the vehicle side, which will unlock the door or not depending on detecting irregularities, working as an intrusion detection system.

Similarly to this work and extending the fingerprinting technique to the key fob, we have *HODOR* [57], also along with a separate paper analyzing the solution with a real-world setup [56]. The paper presents a new formal attack model that covers both RKE and PKES systems. In this model, the fingerprinting method aims to identify legitimate key fobs while detecting bad actors. HODOR runs on an external device that can capture and analyze packets on UHF band without modifying the commercial key fobs already on the market. The fingerprinting technique extracts the signal features from the pulse preamble: the peak frequency, the carrier frequency offset, the Signal-to-Noise Ration (SNR), and other statistical features. From the data, HODOR requires a training phase for the classifier that categorizes a signal as if it is from an attacker. In addition, HODOR can handle different environmental factors that could affect the classification. The results are promising, but the authors argue that the proposed method is still insufficient for practical use.

In the literature and other media, we also find suggestions to mitigate the replay and relay attacks, such as in [41], where a first short-term suggestion is to shield the key fob to avoid relay. Drastically, the authors also proposed to remove the battery from the device. Other solutions advise rolling back to physical locks or deactivating the remote entry (if the vehicle allows it) to reactivate it the next time the driver approaches the car [23].

To conclude, the defense side must also cope with the new threats on web and car connectivity. In this case, the defender is at a disadvantage due to the high complexity of the systems and the need to secure everything to an attack that only needs one entry point.

7 Attacks And Defenses Takeaways

After presenting the different attacks and defenses proposed by security researchers over the years, we analyze the current situation in the automotive scenario regarding RKE and PKES systems. In this section, we answer the first three questions regarding the changes in the attack types and the overall security of the RKE (Question 1 and Question 2). Then, we answer Question 3, analyzing the effectiveness of the defense mechanisms proposed and their deployment in the real world. However, we can only make an analysis based on public information due to the close source systems of car manufacturers. Based on the research carried out in this paper, we deduce that

> *A1. The RKE and PKES systems are generally more secure thanks to their evolution in technology and techniques.*

Nonetheless, the security regards principally the hardening against the cryptographic functions and the difficulty in reverse engineering the newly adopted systems such as BLE and NFC. Additionally, adopting regulations will positively impact the general security of these devices. This does not mean breaking them is impossible, as we saw in the attack section. On the contrary, vulnerabilities in new systems let attackers perform malicious actions more freely without the need for user interaction or noticing. Furthermore, new technologies, such as web services and BLE, enlarge the attack surface. To conclude this answer, the RKE systems available also now could integrate older technologies (even fixed code) and still be vulnerable to most of the attacks presented in this paper [27]. In general, the RKE systems have better security mechanisms in place to defend against typical cryptographic attacks but still lack security against relay and replay attacks, which are still a threat to these devices. The physical layer attacks are more complex to defend against, leading the shift to new technologies such as UWB. This brings us directly to answering the second question:

> *A2. The attack types did not change during the last 15 years. This is mostly due to the relay attack's exploitability, ease, and diffusion [3].*

In fact, as anticipated in Section 4, in legacy technologies, the focus was on cryptographic operations, but the physical layer remained the same. This allowed the attackers to exploit RollJam and relay attacks in more advanced systems. In fact, the jamming and replay attack is still a viable option for the thieves. The hardening in the cryptographic functions made cryptographic attacks harder to perform. However, the relay is still possible even in BLE and NFC technologies, as we discussed in Section 5. Above all, the UWB promises of relay protection are in discussion in this last year due to possible attacks against such systems [4]. Moreover, the introduction of web services and API brought a new paradigm in the automotive scenario with the need to adapt the defenses and security measures to a broader scope.

Regarding the effectiveness of the defenses, we can infer that it is harder to exploit cryptographic weaknesses or find them in the wild. However, we can infer that:

> *A3. All the different proposals found in the literature are not implemented in real systems, thus reducing the effectiveness of the defense methods developed by the academic research.*

The motivation must be found in the developing of schemes that require various hardware and software implementation, with maintenance by the car manufacturers. Additionally, as we show in Table 3, in general, these works miss effective and real studies on the possible implementations and computational costs they have on the system. Only a few of them

consider the cost of introducing new protocols. Still, Joo et al. considered the 500 ms threshold admissible due to the difficulty for a human to notice any difference [56]. Also, the development costs for RKE systems can rise due to the dedicated hardware needed for the proposed systems, which can discourage companies from adopting such methods. Moreover, different proposed techniques did not have a real-world study case or experimentation, supporting their results based only on simulations, thus not impacting the choices of OEMs in adopting such countermeasures. To conclude, most works attempt to contrast the Relay and RollJam attacks. The different assumptions and hardware setups affect the possible deployability, especially when considering a setup phase that uses a PUF-based or QKD-based protocols [72, 74] that need special hardware and secure channels with trusted nodes.

8 Future Directions

The research in RKE and PKES system security is gaining ground in the automotive scenario, and it is needed to keep our cars secure from thieves. The answer to the last research question is as follows:

> *A4. Car manufacturers used the security-by-obscurity paradigm to prevent attacks. The change in this mentality will strengthen the RKE and PKES technology, with the cooperation of security researchers and more open specifications and details of such technologies.*

In research and development, the study and adoption of UWB is promising but needs more robust implementations to protect against relay attacks. However, to achieve this result, we need companies to trust the security community and seek more security auditing and testing, especially now that web vulnerabilities are much easier to introduce in complex systems. First, the open source paradigm can offer transparency, faster security updates, and an entire community searching for bugs and patching vulnerabilities. On the contrary, closed-source development, generally adopted by companies, relies only on the black-box approach from the attacker's perspective, but different examples in various environments show how this approach is fallacious. A good starting point is what we saw last year, and it has already been replicated for 2025 with the introduction of the Pwn2Own Automotive competition, where companies and the best security researchers meet to test the latest technologies [10]. Regarding academic research, the new focus should target the web applications and APIs, with new methods to precisely tailor the automotive case studies and find possible vulnerabilities and wrong paradigms assumed by the developers. In addition, UWB, Bluetooth, and NFC technologies can still be a valuable research direction to stress out due to the technical difficulties in following the specifications without introducing errors. The use of standards and normative helps in developing new RKE systems

that are secure against known attacks. In fact, as discussed in Section 3, the ISO/SAE 21434 provides guidelines to build a secure system only as requirements and not on how to implement it with specific technical characteristics. The presence of a specific standardization and technology to use in creating RKE system can thus provide better regulations for OEMs. At the same time, there is also the need for more agencies to assist at the developing stage and control the conformity to the regulations.

9 Related Works

Only a few works tried to assess the security and point out the current situation about RKE and PKES systems. Most manuscripts include them in a broader discussion about a comprehensive automotive security review, indicating remote entry as an attack surface [33, 54, 85]. Among the RKE specific works, Tillich and Wójcik presented a study on a particular car immobilizer application by Amtel, implementing an open security protocol stack [82]. The authors described the five theoretical attacks they found against it without implementation. Only two works comprehensively review the technologies utilized in vehicle remote access. The first one presents a security analysis and replication of simple attacks by Breuls [31]. In the thesis manuscript, the author describes the history of the remote keyless entry, provides a general representation, and provides a specific case of KeeLoq in Microchip Technology. After that, the author implements the Jamming and Replay attack with a detailed technical description. The second and most recent, by Zheng et al. [98], is similar to this work but only discusses the technologies in a high-level overview, briefly presenting some of the most well-known attacks. Furthermore, it does not cover the new technologies and web application interface for remote keyless entry. Nonetheless, the authors present a good overview of these systems, especially regarding defense mechanisms.

10 Conclusions

This work presented the first comprehensive systematic review of attacks and defenses tailoring remote keyless vehicle entry. The goal of this systematization of knowledge is to assess the situation nudging the evolution of the RKE during the years and how attacks have afflicted it that persist still now. We described the attack classes on different technologies in such systems and how researchers tried to cope with them, presenting various solutions. We analyzed the problems that brought to the current state, with relay and RollJam as a threat to even the most advanced RKE systems, and how the web services enlarged the attack surface. Finally, we hint at the topics researchers can follow to make these systems more secure.

References

[1] Add your car key to Apple Wallet on your iPhone or Apple Watch.

[2] Car API - The developer friendly vehicle API & database.

[3] Chasing Cars: Keyless Entry System Attacks.

[4] From Key Fob to UWB: How Hackers Hijack Vehicle Entry Systems.

[5] Get an Easier, Safer Key with Digital Car Key.

[6] How a Hacker Controlled Dozens of Teslas Using a Flaw in Third-Party App.

[7] Report: Why drivers are turning to third-party car apps · Smartcar blog.

[8] Tesla API | Tesla API.

[9] What's the deal with Ultra Wideband technology and what will it do for your car? | BMW.com.

[10] The World's Largest Zero-Day Vulnerability Discovery Contest to Be Held in Japan Once Again Next Year.

[11] 'The issue is significant': Experts issue keyless car theft warning.

[12] 'The issue is significant': Experts issue keyless car theft warning.

[13] Automobile-theft preventer. *Google Patents*, 8, April 1936.

[14] Technical specifications. *NFC Forum. Archived from the original on*, 4, August 2011.

[15] Keyless wonder: how did we end up with "smart" keys for our cars?, November 2014.

[16] Jam and Replay Attacks on Vehicular Keyless Entry Systems, July 2019.

[17] BMW announces BMW Digital Key Plus with Ultra-Wideband technology coming to the BMW iX., 2021.

[18] Rolling PWN, 2022.

[19] Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More, 2023.

[20] Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More, 2023.

[21] Hacking Kia: Remotely Controlling Cars With Just a License Plate, September 2024.

[22] Hacking Kia: Remotely Controlling Cars With Just a License Plate, September 2024.

[23] Protecting your car from growing risk of keyless vehicle thefts, January 2025.

[24] Kevin 2600 and Alex. Hacking TESLA Model 3 - NFC Relay Revisited, August 2020.

[25] Usman Ahmad, Hong Song, Awais Bilal, Mamoun Alazab, and Alireza Jolfaei. Securing smart vehicles from relay attacks using machine learning. *The Journal of Supercomputing*, 76(4):2665–2682, April 2020.

[26] A.I. Alrabady and S.M. Mahmud. Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs. *IEEE Transactions on Vehicular Technology*, 54(1):41–50, 2005.

[27] Rajesh Ayyappan. Security like the 80s: How I stole your RF, August 2022.

[28] Ryad Benadjila, Mathieu Renard, José Lopes-Esteves, and Chaouki Kasmi. One car, two frames: Attacks on hitag-2 remote keyless entry systems revisited. In *11th USENIX Workshop on Offensive Technologies (WOOT 17)*, Vancouver, BC, August 2017. USENIX Association.

[29] Andrey Bogdanov. Attacks on the keeloq block cipher and authentication systems. 2007.

[30] Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, and Michael Szydlo. Security analysis of a Cryptographically-Enabled RFID device. In *14th USENIX Security Symposium (USENIX Security 05)*, Baltimore, MD, July 2005. USENIX Association.

[31] Jordi Breuls. Security analysis and exploitations of keyless entry systems in cars. 2019.

[32] Car Hacking Village. Remote Exploitation of Honda Cars, August 2022.

[33] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *20th USENIX Security Symposium (USENIX Security 11)*, San Francisco, CA, August 2011. USENIX Association.

[34] Nicolas T. Courtois, Gregory V. Bard, and David Wagner. Algebraic and slide attacks on keeloq. In Kaisa Nyberg, editor, *Fast Software Encryption*, pages 97–115, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[35] Nicolas T. Courtois, Sean O'Neil, and Jean-Jacques Quisquater. Practical algebraic attacks on the hitag2 stream cipher. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio A. Ardagna, editors, *Information Security*, pages 167–176, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[36] Levente Csikor, Hoon Wei Lim, Jun Wen Wong, Soundarya Ramesh, Rohini Poolat Parameswarath, and Mun Choon Chan. Rollback: A new time-agnostic replay attack against the automotive remote keyless entry systems. *ACM Trans. Cyber-Phys. Syst.*, 8(1), January 2024.

[37] Zachary Depp, Halit Bugra Tulay, and C. Emre Koksal. Enhanced Vehicular Roll-Jam Attack using a Known Noise Source. In *Proceedings Inaugural International Symposium on Vehicle Security & Privacy*, San Diego, CA, USA, 2023. Internet Society.

[38] Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani. On the power of power analysis in the real world: A complete break of the keeloq code hopping scheme. In David Wagner, editor, *Advances in Cryptology – CRYPTO 2008*, pages 203–220, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[39] fmsh seclab. fmsh-seclab/TesMla, July 2024. original-date: 2022-06-09T13:04:41Z.

[40] International Organization for Standardization. Iso/sae 21434:2021 road vehicles — cybersecurity engineering. 2021.

[41] Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, February 6-9*, 2011.

[42] Flavio D. Garcia, David Oswald, Timo Kasper, and Pierre Pavlidès. Lock it and still lose it —on the (In)Security of automotive remote keyless entry systems. In *25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX, August 2016. USENIX Association.

[43] Tobias Glocker, Timo Mantere, and Mohammed Elmusrati. A protocol for a secure remote keyless entry system applicable in vehicles using symmetric-key cryptography. In *2017 8th International Conference on Information and Communication Systems (ICICS)*, pages 310–315, 2017.

[44] Andy Greenberg. Teslas Can Still Be Stolen With a Cheap Radio Hack—Despite New Keyless Tech. *Wired*.

[45] Andy Greenberg. Teslas Can Still Be Stolen With a Cheap Radio Hack—Despite New Keyless Tech. *Wired*. Section: tags.

[46] Kyle Greene, Deven Rodgers, Henry Dykhuizen, Kyle McNeil, Quamar Niyaz, and Khair Al Shamaileh. Timestamp-based defense mechanism against replay attack in remote keyless entry systems. In *2020 IEEE International Conference on Consumer Electronics (ICCE)*, pages 1–4, 2020.

[47] E. K. Grossman, Thomas J. Watson IBM Research Center Research Division, and B. Tuckerman. *Analysis of a Feistel-like Cipher Weakened by Having No Rotating Key*. IBM Thomas J. Watson Research Division, 1977.

[48] Omar Adel Ibrahim, Ahmed Mohamed Hussain, Gabriele Oligeri, and Roberto Di Pietro. Key is in the air: Hacking remote keyless entry systems. In Brahim Hamid, Barbara Gallina, Asaf Shabtai, Yuval Elovici, and Joaquin Garcia-Alfaro, editors, *Security and Safety Interplay of Intelligent Software Systems*, pages 125–132, Cham, 2019. Springer International Publishing.

[49] Sebastiaan Indesteege, Nathan Keller, Orr Dunkelman, Eli Biham, and Bart Preneel. A practical attack on keeloq. In Nigel Smart, editor, *Advances in Cryptology – EUROCRYPT 2008*, pages 1–18, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[50] European Telecommunications Standards Institute. Electromagnetic compatibility and radio spectrum matters (erm); short range devices (srd); close range inductive data communication equipment operating at 13,56 mhz. 2005.

[51] European Telecommunications Standards Institute. Short range devices (srd) operating in the frequency range 25 mhz to 1 000 mhz. 2018.

[52] Texas Instruments. Digital signal transponder with DST80 authentication, EEPROM, and LF immobilizer, 2012.

[53] Hyera Jeong and Jaewoo So. Channel correlation-based relay attack avoidance in vehicle keyless-entry systems. *Electronics Letters*, 54(6):395–397, 2018.

[54] Pengfei Jing, Zhiqiang Cai, Yingjie Cao, Le Yu, Yuefeng Du, Wenkai Zhang, Chenxiong Qian, Xiapu Luo, Sen Nie, and Shi Wu. Revisiting Automotive Attack Surfaces: a Practitioners' Perspective . In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 2348–2365, Los Alamitos, CA, USA, May 2024. IEEE Computer Society.

[55] Jmaxxz. DEFCON-27-Jmaxxz-Your-Car-is-My-Car, 2019.

[56] Kyungho Joo, Wonsuk Choi, and Dong Hoon Lee. Experimental Analyses of RF Fingerprint Technique for Securing Keyless Entry System in Modern Cars. In *Proceedings 2020 Learning from Authoritative Security Experiment Results Workshop*, San Diego, CA, 2020. Internet Society.

[57] Kyungho Joo, Wonsuk Choi, and Dong Hoon Lee. Hold the Door! Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft. In *Proceedings 2020 Network and Distributed System Security Symposium*, San Diego, CA, 2020. Internet Society.

[58] Markus Kasper, Timo Kasper, Amir Moradi, and Christof Paar. Breaking keeloq in a flash: On extracting keys at lightning speed. In Bart Preneel, editor, *Progress in Cryptology – AFRICACRYPT 2009*, pages 403–420, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[59] Sultan Khan. Technical advisory – tesla ble phone-as-a-key passive entry vulnerable to relay attacks.

[60] Patrick Leu, Giovanni Camurati, Alexander Heinrich, Marc Roeschlin, Claudio Anliker, Matthias Hollick, Srdjan Capkun, and Jiska Classen. Ghost peak: Practical distance reduction attacks against HRP UWB ranging. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1343–1359, Boston, MA, August 2022. USENIX Association.

[61] Csikor Levente and Lim Hoon Wei. BlackHat 2022 USA RollBack Attack. *BlackHat*, 2022.

[62] Paul Lipschutz. Control device for vehicle locks, March 1981.

[63] Kobus Marneweck. An introduction to Keeloq code hopping.

[64] Amir Moradi and Timo Kasper. A new remote keyless entry system resistant to power analysis attacks. In *2009 7th International Conference on Information, Communications and Signal Processing (ICICS)*, pages 1–6, 2009.

[65] The Hacker News. Millions of Vehicles at Risk: API Vulnerabilities Uncovered in 16 Major Car Brands. Section: Article.

[66] The Hacker News. SiriusXM Vulnerability Lets Hackers Remotely Unlock and Start Connected Cars. Section: Article.

[67] The Hacker News. Millions of Vehicles at Risk: API Vulnerabilities Uncovered in 16 Major Car Brands, 2023.

[68] Code of Federal Regulations. Part 15 - radio frequency devices. *Title 47*, 2025.

[69] Association of Radio Industries and Businesses. Arib std-t93: 315 mhz-band telemeter, telecontrol and data transmission radio equipment for specified low power radio station. 2007.

[70] Association of Radio Industries and Businesses. Arib std-t67: 400 mhz-band and 1,200 mhz-band telemeter, telecontrol and data transmission radio equipment for specified low-power radio station. 2019.

[71] David F. Oswald. Wireless attacks on automotive remote keyless entry systems. In *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*, TrustED '16, page 43–44, New York, NY, USA, 2016. Association for Computing Machinery.

[72] Rohini Poolat Parameswarath, Nalam Venkata Abhishek, and Biplab Sikdar. A quantum safe authentication protocol for remote keyless entry systems in cars. In *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, pages 1–7, 2023.

[73] Rohini Poolat Parameswarath and Biplab Sikdar. An authentication mechanism for remote keyless entry systems in cars to prevent replay and rolljam attacks. In *2022 IEEE Intelligent Vehicles Symposium (IV)*, pages 1725–1730, 2022.

[74] Rohini Poolat Parameswarath and Biplab Sikdar. A puf-based lightweight and secure mutual authentication mechanism for remote keyless entry systems. In *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, pages 1776–1781, 2022.

[75] Jinita Patel, Manik Lal Das, and Sukumar Nandi. On the security of remote key less entry for vehicles. In *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pages 1–6, 2018.

[76] Kaaviya Ragupathy. 30+ Tesla Cars Hacked Using Third-Party Software, May 2024.

[77] Kaaviya Ragupathy. 30+ Tesla Cars Hacked Using Third-Party Software, May 2024.

[78] Samy Kamkar. DEF CON 23 - Samy Kamkar - Drive it like you Hacked it: New Attacks and Tools to Wireles, December 2015.

[79] Ritul Satish, Alfred Daimari, Argha Chakrabarty, Kahaan Shah, and Debayan Gupta. Attacking automotive RKE security: How smart are your 'smart' keys? Cryptology ePrint Archive, Paper 2024/1816, 2024.

[80] Mridula Singh, Patrick Leu, and Srdjan Capkun. UWB with Pulse Reordering: Securing Ranging against Relay

and Physical-Layer Attacks. In *Proceedings 2019 Network and Distributed System Security Symposium*, San Diego, CA, 2019. Internet Society.

[81] Tesla. Model 3 owner's manual.

[82] Stefan Tillich and Marcin Wójcik. Security analysis of an open car immobilizer protocol stack. In Chris J. Mitchell and Allan Tomlinson, editors, *Trusted Systems*, pages 83–94, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[83] Jon Ungoed-Thomas. Gone in 20 seconds: how 'smart keys' have fuelled a new wave of car crime. *The Observer*, February 2024.

[84] Colin Urquhart, Xavier Bellekens, Christos Tachtatzis, Robert Atkinson, Hanan Hindy, and Amar Seeam. Cyber-security internals of a skoda octavia vrs: A hands on approach. *IEEE Access*, 7:146057–146069, 2019.

[85] Chris Valasek and Charlie Miller. A Survey of Remote Automotive Attack Surfaces. 2014.

[86] Roel Verdult and Fl Avio D Garcia. Cryptanalysis of the Megamos Crypto Automotive Immobilizer. 40(6), 2015.

[87] Roel Verdult, Flavio D. Garcia, and Josep Balasch. Gone in 360 seconds: Hijacking with hitag2. In *21st USENIX Security Symposium (USENIX Security 12)*, pages 237–252, Bellevue, WA, August 2012. USENIX Association.

[88] Roel Verdult, Flavio D. Garcia, and Baris Ege. Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer. In *22nd USENIX Security Symposium (USENIX Security 13)*, Washington, D.C., August 2013. USENIX Association.

[89] Aram Verstegen, Roel Verdult, and Wouter Bokslag. Hitag 2 hell – brutally optimizing Guess-and-Determine attacks. In *12th USENIX Workshop on Offensive Technologies (WOOT 18)*, Baltimore, MD, August 2018. USENIX Association.

[90] Juan Wang, Karim Lounis, and Mohammad Zulkernine. Cskes: A context-based secure keyless entry system. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, volume 1, pages 817–822, 2019.

[91] I. Wiener. *Philips/NXP Hitag2 PCF7936/46/47/52 stream cipher reference implementation*. http://cryptolib.com/ciphers/hitag2/, 2007.

[92] Lennert Wouters, Benedikt Gierlichs, and Bart Preneel. My other car is your car: compromising the tesla model x keyless entry system. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(4):149–172, Aug. 2021.

[93] Lennert Wouters, Eduard Marin, Tomer Ashur, Benedikt Gierlichs, and Bart Preneel. Fast, furious and insecure: Passive keyless entry and start systems in modern supercars. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(3):66–85, May 2019.

[94] Lennert Wouters, Jan Van den Herrewegen, Flavio D. Garcia, David Oswald, Benedikt Gierlichs, and Bart Preneel. Dismantling dst80-based immobiliser systems. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020(2):99–127, Mar. 2020.

[95] Lennert Woutersa, Jan Van den Herrewegen, Flavio D. Garcia, David Oswald, Benedikt Gierlichs, and Bart Preneel. Dismantling DST80-based Immobiliser Systems. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2020(2):99–127, Mar. 2020.

[96] Xinyi Xie, Kun Jiang, Rui Dai, Jun Lu, Lihui Wang, Qing Li, and Jun Yu. Access Your Tesla without Your Awareness: Compromising Keyless Entry System of Model 3. In *Proceedings 2023 Network and Distributed System Security Symposium*, San Diego, CA, USA, 2023. Internet Society.

[97] Yifan Xie, Hyung June Kim, Sa Yong Chong, and Taek Lyul Song. Time-based countermeasures for relay attacks on pkes systems. In *Proceedings of the 16th International Conference on Informatics in Control, Automation and Robotics - Volume 1: ICINCO*, pages 795–801. INSTICC, SciTePress, 2019.

[98] Yong Zheng, Man Zhang, Xianfeng Li, Xingchi Chen, Zhourui Zhang, Jiaming Zhu, Chun Shan, and Guocheng Wu. Automotive security in the digital era: A comprehensive survey of attacks and defenses for keyless entry system. In Kun Zhou, editor, *Computational and Experimental Simulations in Engineering*, pages 444–467, Cham, 2025. Springer Nature Switzerland.

[99] Petr Štembera and Martin Novotny. Breaking hitag2 with reconfigurable hardware. In *2011 14th Euromicro Conference on Digital System Design*, pages 558–563, 2011.