Design and Security Considerations for Passive Immobilizer Systems

Jim Goings, Toby Prescott, Michael Hahnen, Karl Militzer

For years, consumers have come to rely on the convenience and added security that a passive vehicle immobilizer system offers. These systems consist of a key fob, carried by the driver, and a base station, mounted in the vehicle. They work together to determine if the driver is authorized to start the vehicle. Of equal or greater importance is the system's ability to prevent unauthorized sources from using the vehicle. While top-level functionality of a vehicle immobilizer is simple to describe, the underlying technology enabling it is intriguing and sophisticated. This article will explore both the hardware and software aspects of vehicle immobilizer systems as well as offer noteworthy comments on design and security considerations.

Communication

The prevailing method of communication between key fob and vehicle in passive vehicle immobilizer systems today is with a modulated magnetic field. This field is created by the vehicle's immobilizer base station from a low frequency alternating current, typically 125kHz. The magnetic field serves three fundamental purposes: A) the power source for the key fob, hence the term "passive", B) a carrier on which information from the base station to key fob is conveyed, e.g. "downlink", C) a carrier on which information from the key fob to the base station is conveyed, e.g. "uplink".

Characteristics of magnetic fields that are of particular appeal for a vehicle immobilizer system pertain most to the key fob's need to operate completely passively, e.g. without a battery. "Downlink" field detection and "uplink" field modulation can both be achieved using circuitry that consumes very little current. Furthermore, harnessing sufficient field energy to power these circuits in the key fob electronics can be achieved with relative ease.

During the system design phase, care must be taken to carefully consider key performance parameters such as key fob energy requirements, which affect antenna coil geometries and drive levels, and the authentication process, which has a direct impact on response time. The sections that follow will address these topics in greater detail.

System Interfaces

The system architecture of a vehicle immobilizer has several layers of abstraction, each representing different system interfaces. Figure 1 provides a visual representation of these layers.

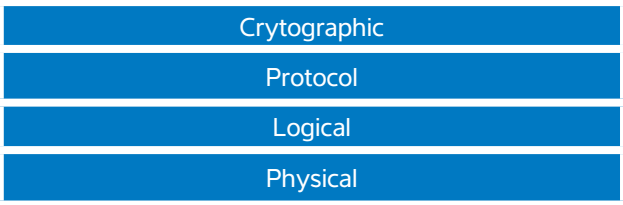

Figure 1. Vehicle Immobilizer Interface Layers

The Physical Layer

A t the lowest level of a vehicle immobilizer system is the physical layer. It consists of a vehicle-mounted antenna coil capable of creating a magnetic field of sufficient magnitude to enable its detection and modulation by an antenna coil mounted in the user's key fob.

Field Generation and Modulation

Vehicle immobilizer systems can be classified in one of two different ways based on how the magnetic field is used to support the transfer data: half duplex or full duplex. In a half-duplex system, the vehicle-mounted antenna coil alternates between periods of energy transfer and data transfer. Uplink data (e.g., fob to vehicle) is modulated using Frequency Shift Keying (FSK). A graphical representation of this communication method is shown in Figure 2. Two points should be intuitively obvious from viewing Figure 2. First, the rate of data transfer suffers from a significant compromise due to the recurring need to perform the energy transfer, e.g., charge up the key fob. Second, the modulated signal is very small compared to the field present during the energy transfer period, making it more susceptible to interference from ambient noise which results in reduced range. These characteristics have caused the popularity of half-duplex systems to wane.

The dominant system in use today is the full-duplex system in which the vehicle-mounted antenna coil performs energy transfer AND data transfer simultaneously. Uplink data is modulated using Amplitude Shift Keying (ASK). A graphical

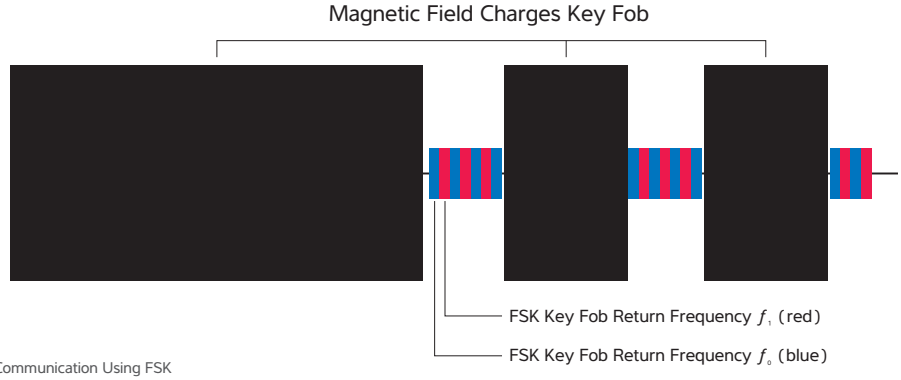

Figure 2. Half-duplex Communication Using FSK

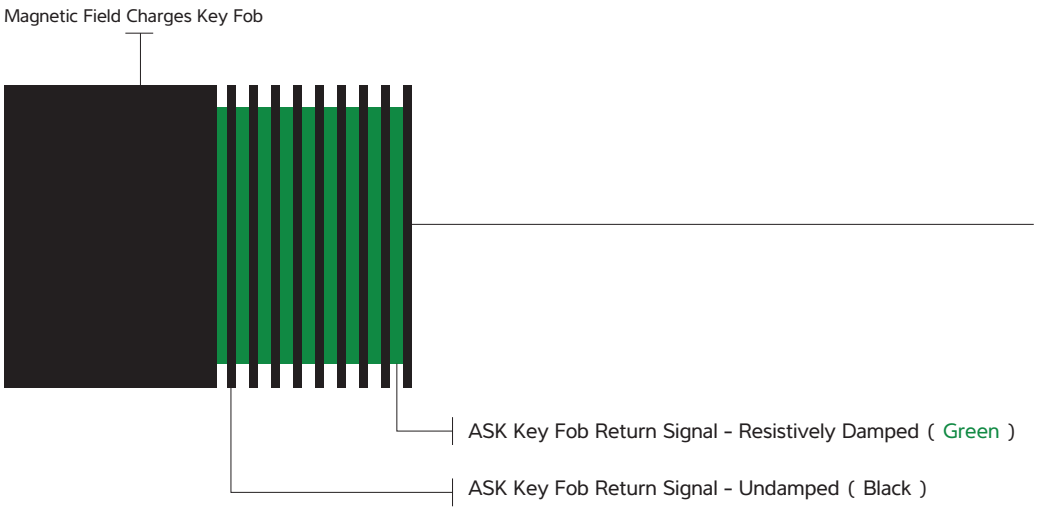

Figure 3. Full-duplex Communication Using ASK

representation of this communication method is shown in Figure 3. Clearly, the ability to simultaneously transfer data while keeping the key fob energized, or charged, provides the design engineer a significant data transfer rate advantage over half-duplex systems. Additionally, the constant carrier field tends to mask out interferences and enables robust communication during the data transfer. Furthermore, this approach can be realized using simple envelope detection circuitry. Because of the popularity of the full-duplex vehicle immobilizer system in the market place today, the rest of this document will focus on this type of system.

System Interfaces: the Logical Layer

The next layer above the physical layer is the logical layer. This layer captures the characteristics and requirements for the coding and transfer of data across the magnetic field. It applies to the bi-directional data transfer that takes place from vehicle to key fob, commonly referred to as "downlink", as well as key fob to vehicle, also known as "uplink".

Downlink

Downlink information is coded using Pulse Length Modulation; typically Binary Pulse Length Modulation (BPLM) or Quad Pulse Length Modulation (QPLM). This method is based on inserting a carrier field gap, Tgap, of fixed duration and setting the gap to gap timing intervals to predetermined times; T0 for a logic "0" and T1 for a logic "1". The advantage to this approach is that it embeds energy transfer from vehicle to key fob into the data encoding and ensures the key fob will be supplied enough energy to process the encoded data. However, a side effect of this encoding method is that the data transfer baud rate depends on the logical value of the data bit stream being sent since the transmission times for each binary state are different. See Figure 4 for a more detailed graphical depiction of this coding method.

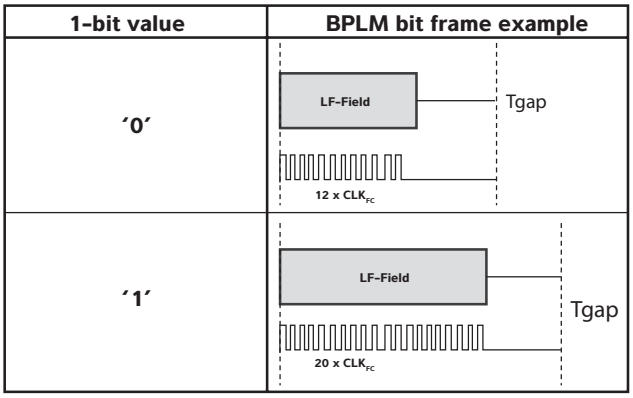

Figure 4. BPLM Coding Method

QPLM is a variation of BPLM that is sometimes used. With this modulation, two bits are transmitted after one gap, and therefore more power is available on the transponder side. In addition, the average baud rate is higher compared to BPLM. The coding method follows the same basic implementation as BPLM, except the allowed number of states is extended from two to four and the predetermined gap to gap timing

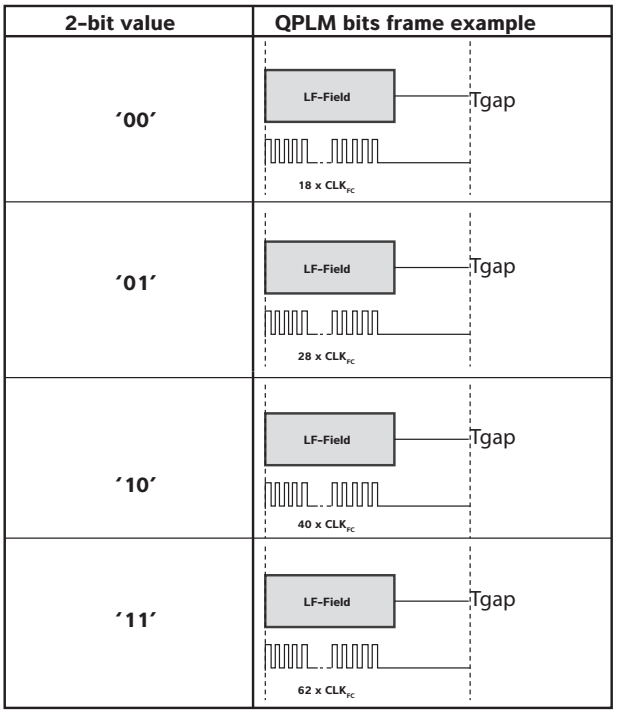

Figure 5. QPLM Coding Method

intervals are expanded to cover the additional states. See Figure 5 for a visual representation of QPLM.

Uplink

Information communicated from the user fob to the vehicle base station is typically encoded using Manchester or Bi-phase. These encoding methods share several characteristics that differ from the downlink: A) the encoded bit stream always has an average duty cycle of 50%, B) the time to send encoded data is based solely on the baud rate.

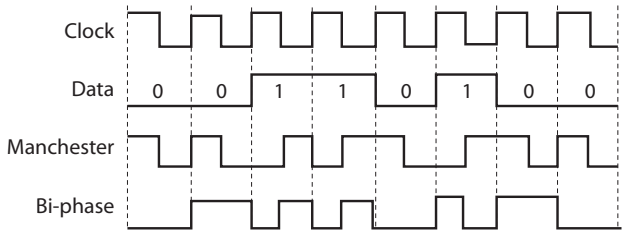

Figure 6. Manchester and Bi-phase Coding

Both encoding techniques enable clock extraction from the encoded data stream. This is possible because all time durations in the coded bit stream are quantized to one of two values; T or 2T, where T is what is referred to as a "half bit". Data rate is fixed by the relationship 1/(2T). Clock extraction merely requires the detection of the minimum time duration element, T, and synchronizing its phase with the coded bit stream.

Protocol Layer

The protocol layer defines how individual data bits are grouped to enable communication between the vehicle base station and key fob. It defines how many bits and in which order they are transmitted between the reader and the transponder. As a simple analogy, this can be compared to the rules governing the formation of sentences in using words. The protocol layer would be like the sentence formed from the logical layer which would be like the words. It forms a fixed set of commands along with their allowable responses.

Authentication

Authentication is the term used to describe the process of deciding whether the driver is authorized to start the vehicle. The simplest form of this is called unilateral authentication. In this case, the vehicle "tests" the key fob to determine if it has been associated/learned to the vehicle. When an additional step is added to this process, in which the key attempts to "test" the vehicle to determine if it has been associated with the key fob, it becomes bilateral or mutual authentication. Clearly, this added step increases security strength but comes at the expense of longer authentication time.

Unilateral Authentication Protocol

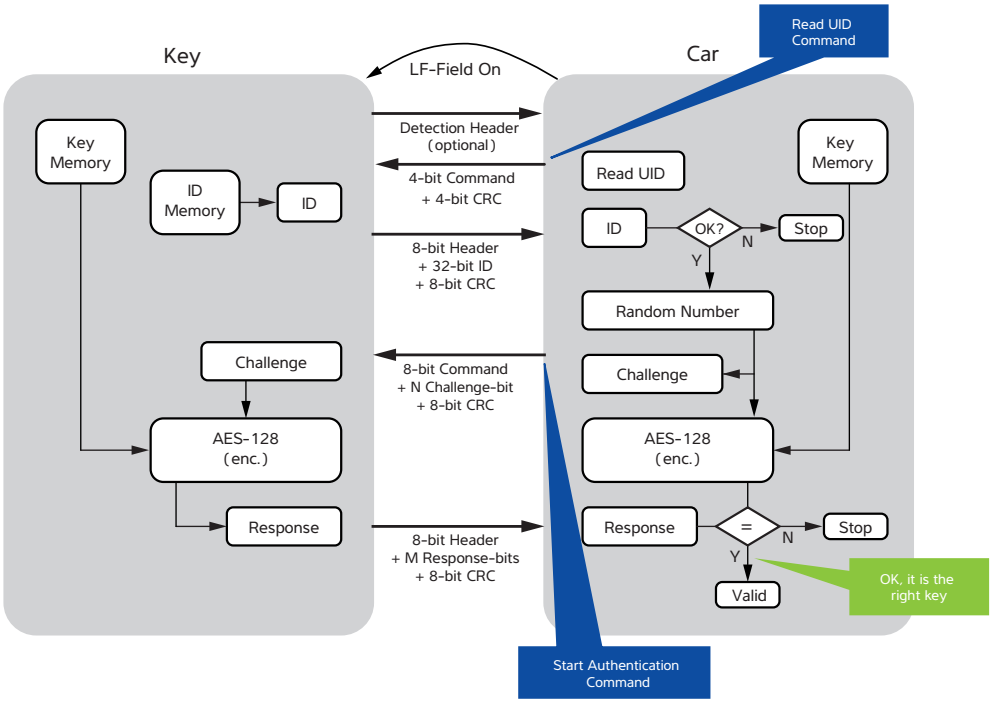

Figure 7. Unilateral Authentication

Unilateral Authentication

Typically, the unilateral authentication protocol is initiated by the vehicle and consists of the following steps:

1. Vehicle reads the key fob's unique ID (not to be confused with the secret key)
2. Vehicle generates a random number challenge and sends it to the key fob
3. Key fob encrypts the challenge (using the secret key) and sends this response to the vehicle
4. Vehicle compares key fob's response with its calculated response (using same key and challenge)

Note: The vehicle must posses the key fob's secret key to enable the success of this transaction. The process of sharing the secret key is called "Key Learn" and is described in the next section.

Key Learn: Open/ Secure

The Key Learn Protocol is the process that is used to allow the vehicle to establish a secret key and share it with the key fob. Depending on the restrictions and safeguards placed on the initiated Key Learn session by the vehicle, secret keys can be shared openly or securely.

An open Key Learn process would typically consist of the following steps, also shown in Figure 8:

1. Vehicle generates a secret key based on a random number and "proposes" it to the key fob
2. Key fob "accepts" secret key, saves to memory, and responds with an acknowledgment
3. Vehicle saves secret key to memory after successful receipt of key fob's acknowledgement

If the Key Learn Protocol can't be protected from eavesdroppers or unauthorized access to the vehicle, it may be desirable to utilize a Secure Key Learn Process.

Open Key Learn 1/2

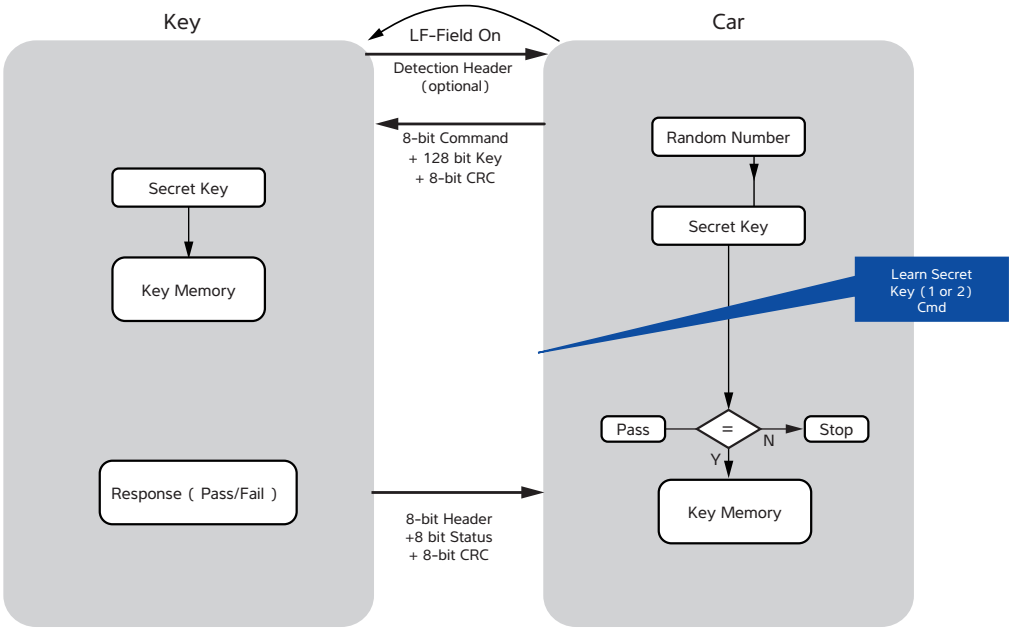

Figure 8. Open Key Learn

Bilateral or Quasi-mutual Authentication

A more complex form of an authentication process is the quasi-mutual or bilateral authentication. It is not a full mutual authentication that is implemented in the Atmel® immobilizer system because it does not use random generators on both sides of the system, the car and the key. The implemented solution uses a MAC (Message Authentication Code) to authenticate the car vis-à-vis the key.

Again, the authentication protocol is initiated by the vehicle and – in case of a bilateral authentication –consists of the following steps as shown in Figure 9:

1. Vehicle reads the key fob's unique ID
2. Vehicle generates a random number challenge and sends it to the key fob
3. Vehicle encrypts the random number and appends it to the challenge
4. Key fob encrypts the challenge (using secret key 1) and compares it with the received encrypted challenge (MAC)
5. If the result matches, the key fob encrypts it (using secret key 2) and sends this response to the vehicle
6. Vehicle compares key fob's response with its calculated response (using same key and challenge)

Cryptographic Layer

The cryptographic layer provides the highest level of encryption. It contains the mathematical function that transforms a plain text message into a secret message. Ideally, this function should have two properties:

1. Unique: For every plain text input, there must be a unique secret text output
2. Unpredictable: It must not be possible to predict a plain text to secret text pair, even if a large sample of known good plain text to secret text pairs was available for analysis

Bilateral Authentication Protocol

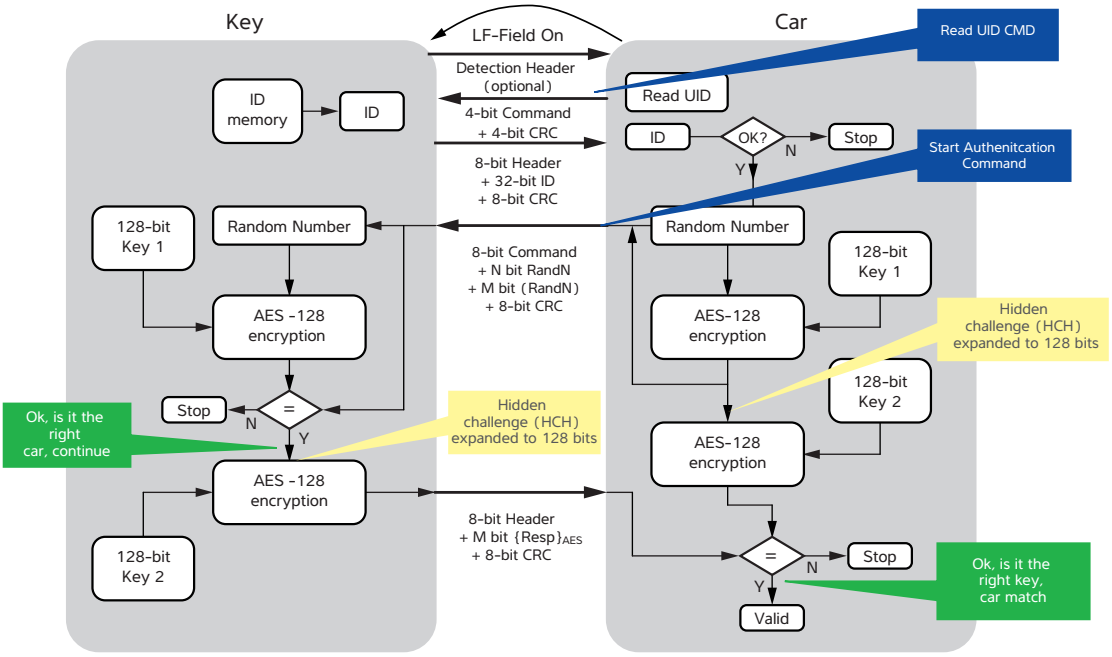

Figure 9. Bilateral Authentication Protocol

Public vs. Private

For many years, private cryptographic algorithms were commonplace. However, private algorithms have drawbacks: A) uncertainty of algorithm's strength, B) lack of being subjected to critical peer review, C) potential wide-scale security compromise should the algorithm be leaked to the public. In recent years, several high-profile examples can be cited that illustrate these weaknesses. Perhaps even more compelling is the lack of interoperability in systems that share the same physical and logical layers. This interferes with basic competitive market forces and in many cases drives higher system costs.

In an effort to address these concerns, public opinion has shifted toward the acceptance of a public domain encryption algorithm – the Advanced Encryption Standard (or AES, as it is more commonly referred to). Its origin comes from the 1997 initiative at the National Institute of Standards and Technology (NIST) to select a public-domain encryption algorithm. Within a year, fifteen candidate algorithms were identified and subjected to critical review by the cryptographic research community. This analysis included an assessment of security and efficiency characteristics for each algorithm. After trimming the list of candidates from fifteen to four, NIST subjected them to a second round of public review before finally selecting the AES algorithm in 2000.

AES, as we know it today, is a symmetrical block cipher that combines a 128-bit plain text input with a 128-bit secret key to create a 128-bit encrypted output. Due to its symmetrical characteristics, AES can also be used in reverse to combine the encrypted output with the secret key to find and extract the original plain text input.

System Security Considerations – Attacks and Countermeasures

A common misconception held today is that the security of a vehicle immobilizer system is established by the strength of the encryption algorithm. While encryption algorithm strength is important, it alone does not define the overall system's resistance to attack. Each of the interface layers in the immobilizer system, algorithmic, protocol, logical and physical, contributes to the system's overall security and must be studied and fortified against attack.

Algorithmic Security and Countermeasures

As noted earlier, it is imperative that the encryption algorithm possess unique and unpredictable characteristics. In the case of AES, the details of how the algorithm operates is freely available to the public and as a result, it has been subject to critical review by the research community. This, by far, is the best countermeasure available. To date, scientific studies have confirmed the algorithm's strength as it has withstood the test of time (over 10 years). However, in the case of private algorithms, scientific analysis by the research community was not possible, leaving the strength of these algorithms in question. In fact, many have failed to withstand the test of time and in recent years their weaknesses have been exposed.

Protocol Security and Countermeasures

In systems using unilateral authentication, attacks on the protocol layer are typically accomplished using "scan" or "dictionary" methods. In a "scan" attack, the attacker receives a challenge from the vehicle and returns random values in response. If the protocol consisted of a 56-bit response, then the bit security is 2^{56} , i.e., it takes 2^{56} trials to get one valid challenge-response pair. To resist this type of attack, the following measures can be considered:

- Increasing the response bit length to add complexity
- Having the vehicle embed exponentially growing time-outs between consecutive unsuccessful trials
- Having the vehicle block trials after a fixed number of consecutive unsuccessful trials are attempted

In a "dictionary" attack, the attacker collects valid challenge (from the attacker) response (from the key fob) pairs by communicating directly with the transponder. These pairs are placed in a look-up table or "dictionary" for future reference. Equipped with this dictionary, the attacker then sequentially triggers the vehicle for a challenge, which can be checked in the dictionary for a valid response. If the protocol included a 100-bit response, one would need 2^{51} trials to get one valid challenge-response pair. The "birthday paradox" states that after $2^{n/2}$ logged challenge-response pairs and $2^{n/2}$ trials, the probability of a valid result is 0.5. Using this, it can be shown that the overall complexity of this attack is $2^{n/2+1} = 2^{51}$. Countermeasures to consider in this case are:

- Increasing the challenge bit length to add complexity
- Implementing a bilateral authentication protocol

Physical/Logical Security and Countermeasures

In recent years, attack methods have grown more sophisticated. "Side-channel" attacks such as Simple Power Analysis (SPA) and Differential Power Analysis (DPA) as well as other "invasive" attacks have been successfully applied to extract secret keys from key fobs. These so-called side-channel attacks measure and evaluate the power consumption of a cryptographic device and combine it with knowledge of the plain text or cipher text in order to extract an otherwise secret key. The theory underlying these methods is quite sophisticated and beyond the scope of this document. The strongest defense against the side-channel attacks noted above are:

- Randomization of clock frequency and operation
- Interleaving of digital control and the encryption operation

"Invasive" attacks dwell on the physical implementation of the encryption-related circuitry on the silicon die itself. The best countermeasures are fairly simple to implement as long as they are considered early in the design process. The following are examples of steps that could be considered:

- Metal shielding of memory blocks
- Using non-standard synthesis libraries
- Scrambling the location of critical digital elements used during encryption
- Restricting memory access and automatic chip-erase function if attempted

System Performance Considerations

Current Consumption

System performance has different aspects. One is the power consumption of the key fob. This parameter relates directly to the achievable communication distance between key fob and vehicle base station. Car manufacturers and Tier1 suppliers tend to emphasize the importance of the coupling factor as a critical system parameter. However, it mainly represents the relationship of the mechanical dimensions between the key fob's antenna and the vehicle base station's antenna. This parameter is only valid for a given system configuration and depends on antenna inductance, Q-factor, driver current, reader sensitivity, and ignition lock cylinder material. Because of this, use of this parameter alone to compare different systems is inadequate. Of equal if not more importance than the coupling factor is current consumption, especially given that the key side current consumption is a limiting factor in a passive, batteryless environment where

the energy is harvested from a magnetic field and stored in a small capacitor. By selecting system components designed for extremely low power consumption and microcontrollers capable of being programmed with well-balanced software (putting the controller in sleep mode whenever possible), the engineer is able to overcome earlier system disadvantages requiring high coupling factors to compensate for high current consumption in the key fob.

Authentication Response Time

Another important factor in immobilizer systems is the time it takes from turning the key fob inserted inside the lock until the engine starts. This time should be short enough to avoid the driver's perception of a delay. Depending on mechanical and electrical system design and how quick a person can introduce and turn the key, an overall timing budget in the range of 300ms to 500ms is typically available. A significant part of this budget is consumed through mechanics and overhead in the body control module. What remains is between 100ms and 200ms for the authentication process. A good compromise in terms of speed and security seems to be a bilateral authentication with a challenge length of 100 bits and a response length of 56 bits. In most systems this results in a response time of under 100ms.

Error Handling

In case an authentication failed for whatever reason, today's systems require the complete authentication cycle to restart from the beginning and allowing a maximum of three retries within a reasonable time. The retry strategy from Atmel® looks a bit different and enables the system to recover from communication errors more quickly. All commands and optionally the data are protected by a Cyclic Redundancy Check (CRC). Both the key fob and the base station can make use of the CRC to detect errors and signal these conditions to their respective communication partner. This enables the base station to be selective about the amount of repeated info, the last action, the last response, or the last command. This feature enables quicker communication recovery and more attempts at communication recovery in the same amount of time (five-seven retries instead of three).

Summary

By selecting system components that meet the security and performance expectations of the automotive market place, and support a highly configurable and open-source immobilizer software stack, the task of developing a robust vehicle immobilizer system can be greatly simplified. As a leader in automotive vehicle access solutions, Atmel offers such a complete system solution consisting of both hardware and software.

Key fob designs can be realized with the Atmel ATA5580 and the Atmel ATA5795. These devices boast an LF front end, an AES hardware block to perform fast and efficient encryption calculations, coupled with an Atmel AVR® microcontroller that has been optimized for extremely low current operation. Both include programmable flash memory that can be used to run the Atmel open immobilizer protocol or other customer-specific software and are capable of completely passive immobilizer operation.

A base station can be realized with the Atmel ATA5272. This device integrates the LF base-station function with an AVR microcontroller with 8K of programmable flash memory.

As a final complement to these devices, the open immobilizer protocol software from Atmel is available to users at no cost. It provides an unprecedented level of configurability including many user selectable features enabling the dynamic evaluation of system parametric tradeoffs and accelerates the development and optimization process:

1. A logical layer with uplink and downlink baud rate, bit encoding, and modulation depth
2. A protocol layer with challenge and response bit lengths, unilateral or bilateral authentication, data field CRC, two secret keys, secure or open Key Learn
3. A cryptographic layer with AES crypto clock speed from 125 kHz to 4 MHz "on the fly"