Latest Generation Technology for Immobilizer Systems

1. Abstract

Since the introduction of immobilizer systems the need for improved security constantly increases. Many Anti Theft Systems make use of Radio Frequency Identification (RFID) technology because of its unique features. RFID transponders can provide a high level of security at low cost.
This article describes the system approaches for the first and second generation of immobilizer systems. It compares the various security levels and gives an overview about the latest generation technology, called crypto-transponders.

2. Introduction

During 1993 the worldwide increases in automotive theft reached a level which was no longer acceptable for insurance companies. The German insurance companies forced the rapid introduction of a new form of security systems - immobilizers. In other regions various forces such as government agencies also started placing more emphasis on vehicle security.
During a short time frame the automotive industry developed various systems to prevent thieves from entering and/or starting the vehicle. The methods chosen vary from country to country depending on consumer preferences. Remote keyless entry for example is preferred in the USA and in France whereas transparent systems are widely spread in the German market. Due to the unique features of RFID and due to the fact that this technology was already existing for industrial applications, most of the automotive industry decided to make use of small batteryless transponders which offer a high level of security at low cost.
Since the beginning of 1995 nearly all models for the European market are equipped with OEM immobilizers. First statistical analysis of insurance companies in Germany [1] confirm the tremendous success of these systems. Thefts of vehicles with electronic immobilizers decreased to about one tenth compared to vehicles without immobilizer.
However criminal organizations have the means and the resources to develop high sophisticated equipment to overcome existing systems. Constant improvement of the security architecture is necessary to be one step ahead. This article describes the different security levels of key-based immobilizers

and presents the new crypto-transponder generation which offers the highest level of RFID security.

3. Immobilizer System Overview

Key-based immobilizer systems consist of four main components. The core of the system is the *transponder*, a batteryless device which is available in various form factors and with different functionalities. For operation, the transponder has to be supplied with energy from an external source. The *transceiver* generates a high frequency magnetic field which is radiated by an *antenna* coil. The energy activates the transponder and it sends a data stream in form of a modulated RF signal. This signal is demodulated by the transceiver and then passed to the *controller* for data processing.
Different physical principles for RFID systems have been established on the market. Concerning the transmission of energy, two different systems can be distinguished.

- **Full Duplex Systems.** The energy for the transponder and the data signal generated by the transponder are transmitted at the same time, usually using load modulation.

- **Half Duplex Systems.** The transmission of the energy for the transponder and the data signal from the transponder are transmitted consecutively. The transponder stores energy in a capacitor and as soon as the transmitter is switched off, the energy is used to transmit data.

The different techniques have an impact on system design and reading range respectively reliability in the application, but have no impact on the system security.

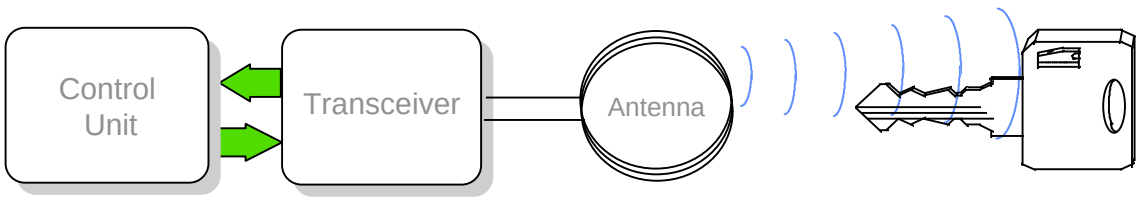

Figure 1: System Block Diagram

4. Cryptographic Background

From the cryptographic point of view, the problem of immobilization consists of two different tasks, the *identification* of the driver and proving his identity, the *authentication*. Several cryptographic means are applicable for driver authentication [2]:

Knowledge
The authentication is based on the knowledge of a secret, for example a password or PIN (Personal Identification Number) that has to be presented to proof the identity. For automotive applications any method using a keyboard is unacceptable for most of the users. In addition the level of security is unacceptable.

Biometrics
Biological attributes, such as fingerprints, voice, retinal or face patterns could theoretically be used for authentication of the driver. However, the technical effort for such systems is still high compared to key-based immobilizers and not acceptable for automotive applications. In addition, the problem of renting a car to someone else and emergency use of a vehicle becomes a critical issue.

Possession
Authentication by means of possession is the most common method and will also be widely spread in future. The simplest implementation is the possession of a mechanical key. A much higher security is offered if the key contains an electronic tag such as a transponder. To start the vehicle, the mechanical key *and* the code in the transponder must match.

All cryptographic systems described above are based on static authentication procedures, that means the security system of the car can verify the identity of the key but the electronics in the key cannot check the identity of the communication partner. A ***mutual authentication*** procedure which also allows the key to verify the identity of the communication partner is one feature that would improve the security level of the system.

A much higher level of security can be achieved with a simple symmetrical algorithm known as ***challenge / response*** protocol. The security system of the vehicle can check the identity of the key by sending a question (a *challenge*) and verifying the answer (*response*). The correct answer can only be given if a secret is known that is shared by both partners. This challenge/response concept has several advantages. During normal use, the secret is not exchanged and both challenge and response vary from cycle to cycle.

5. Standard Security Architectures using RFID

Various security systems using RFID transponders have been established on the market.

Fixed Code Systems. These systems are the most commonly used. During initialization, the controller learns different identification codes stored in the transponders that belong to a vehicle. When the driver places the ignition key in the lock cylinder, the fixed code in the transponder is read and compared to the codes stored in the memory of the controller.
The level of security depends to a great extend on the type of transponder used. There are write once transponders on the market which are delivered

unprogrammed. Programming is done by the user. Commercially available readers/writers allow to pick up the code in the transponder while away from the vehicle and to program an unprogrammed unit. Thus a copy of the fixed code has been generated which cannot be distinguished from the original.
True Read Only systems on the market are factory programmed with a unique identification number. These systems do not allow copies. However, it is possible to emulate the data signal on the radio frequency level. The effort to design an emulator is considerable and requires RF design knowledge.

Rolling Code Systems operate in the same way as fixed code systems except that the secret code in the key is only valid for a certain period of time, typically from one ignition cycle to the other. The System Security Controller re-programs the transponder (which is a Read/Write type) periodically. The secret is changed, but in terms of cryptographics the procedure is still a static authentication.
To guarantee the reliability of the system, resynchronization procedures have to be implemented in case the transponder programming fails or the transponder is reprogrammed by mistake while away from the vehicle. Especially these procedures for resynchronization are the most critical issues in such systems.

Password Protected Transponders. A simple mutual authentication can be provided by password protected transponders. The transponder will deny access to the secret data information stored in its memory unless a password is presented and thus the identity of the reader proven. The length of the password can vary depending on the required security level.
The password is usually transmitted in plain text and can be picked up or guessed if the transponder is available. Depending on the length of the password, the time to guess the password can vary from several minutes to several years.
A limitation of the system is the total transaction time which can be unacceptable for practical use in the application.

Combined Rolling Code / Password Systems can also be implemented using password protected Secured Read Write Transponders. They provide a higher level of security. Critical issues such as timing and resynchronization are also applicable.

6. Crypto Transponders

Crypto Transponders are the second generation of transponders for use in immobilizers. The new generation of crypto transponders developed by Texas Instruments are based upon the TIRIS ™ half duplex RFID technology and are compatible to all standard RF interfaces of the TIRIS ™ product range.

6.1 System Overview

The **D**igital **S**ignature **T**ransponder (DST) is a crypto device which offers the challenge/ response functionality.

During initialization, the vehicle security system and the transponder exchange a secret encryption key. The key cannot be read out, only the transponder response to a challenge sent by the transceiver can be read.

In a typical application, the vehicle security system generates a 40 bit random number (the challenge), and sends it to the transponder using Pulse Width Modulation (PWM). In the transponder the challenge is shifted into the challenge register. For a short period of time, energy is provided by the transceiver and the encryption logic generates a 24 bit response (signature).

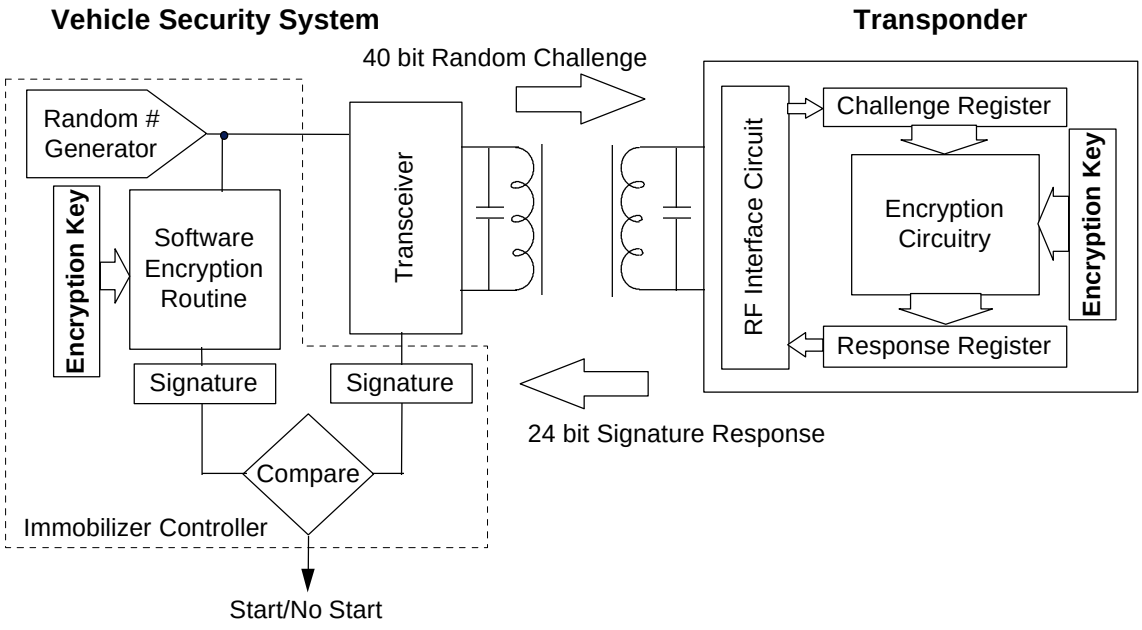

Figure 2: Crypto Transponder System

The response R is a function of the encryption key K_e , the challenge RAND and the cryptographic algorithm F_c .

$$R = f(F_c, RAND, K_e)$$

The response is returned to the transceiver using Frequency Shift Keying (FSK).

The security system calculates the expected response using the same algorithm and the same encryption key and compares the response received from the transponder to the calculated one. The calculation of the expected

response can be done simultaneously to the communication between transponder and reader or after reception of the transponder response. If expected and calculated response are equal, the information is sent to the engine management computer. In time critical applications, the challenge and the response can be generated after immobilization and stored for the next cycle.

The advantages of this system are obvious:

- depending on the challenge the response is different every time. The authentication procedure is dynamic.
- no portion of the encryption key is ever transmitted after initialization of the transponder
- the encryption key cannot be read out
- the transponder cannot be duplicated
- the encryption key can be irreversibly locked or altered if desired.

The transponder is a complex logical and mechanical micro system designed to operate at very low power [3]. During energy transfer less than 1µA is consumed by the transponder IC. This allows a capacitor to be charged over a considerable distance within a reasonable amount of time, typically less than 50ms. Even during the encryption process, the current consumption is below 16µA. Therefore, the typical maximum read range is comparable to standard Read Only systems.

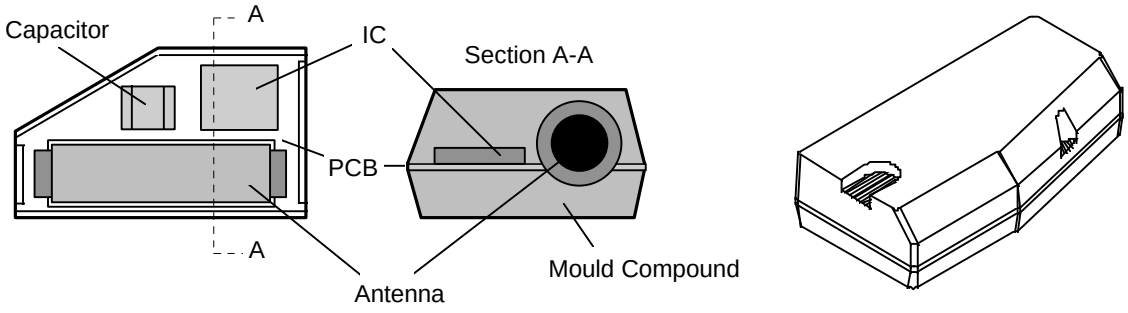

Figure 3: Plastic Wedge Transponder

6.2 Design Objectives

The Digital Signature Transponder was based on many established circuit blocks and assembly techniques to ensure compatibility to existing transceiver hardware and to keep existing qualified automated production lines [4][5][6].

Apart from the design challenges for the IC design:

- maintain low power consumption despite the large number of gates for encryption
- keep wiring of the encryption circuitry to a minimum
- keep chip size to a minimum,

a considerable effort has been spent to ensure

- a high level of cryptographic security
- fast transaction times for the challenge/response cycle
- low data processing effort for the encryption algorithm in the car security system
- reliability in the application in terms of highly sophisticated supervision circuitry in the transponder.

6.3 Encryption

All encryption algorithms are theoretically breakable. An algorithm is *computationally* secure [7] if it cannot be broken within a reasonable amount of time respectively with reasonable resources. In this context 'reasonable' is open to interpretations. Current assumptions for attacks against immobilizer systems are:

- the attacker will not spend more than five minutes in the vehicle
- the key is not longer than ten days available for analysis
- the attacker is familiar with cryptoanalytical techniques.

Scanning is the simplest approach to attack the system. Assuming that the attacker simply transmits a random response to any challenge generated by the security system, the average time to succeed is given by t_s .

$$t_s = R * 2^{(rb-1)}$$

where rb is the length of the response in bit and R is the repetition rate of the security controller in seconds.
Assuming a repetition rate of 200 ms and a response length of 24 bit, the average time to succeed is 19.4 days.

Dictionary attacks can be used if the key was available to the attacker for a certain period of time to build a dictionary of challenge response pairs. In the vehicle, the attacker hopes for a challenge that is already in his dictionary to reply with the correct response and start the engine.
Statistical calculations show that even if the key is available for 10 days and the dictionary is built at a rate of four responses per second, the probability for a successful attack within five minutes in the car is only 0.47%. Taking into

consideration that this effort has to be repeated for each vehicle, it can be understood that this method is uneconomic for the thief.

Cryptoanalysis makes use of the knowledge of the algorithm. Those attackers try to find a mathematical solution to the problem of finding the encryption key with a limited amount of challenge response pairs. The algorithm in the Digital Signature Transponder has been developed to frustrate these cryptoanalytical methods.

6.4 Supervision Circuits

To ensure reliability in the application, several supervision circuits are integrated in the Digital Signature Transponder.
Before the transponder executes a programming or a locking command, several checks have to be passed. These tests are especially important for the locking process, because accidental locking of a page can make the transponder useless. The checks are performed before the internal charge pump is activated to generate the voltage required for programming the EEPROM cells.

A **16 bit Cyclic Redundancy Check (CRC)** according to the CCITT standard is used to check commands, data and addresses that have been received during the write phase. A check of the **correct number of bits** verifies the framing.

During the programming process, the programming voltage must be high enough for a certain amount of time to ensure a reliable programming depth. A Radio Frequency (RF) Limiter is integrated in the transponder to protect the internal IC circuits against overload in case of too high RF fieldstrength applied to the antenna. This limiter is also used for **Programming Supervision**. The saturation of the limiter indicates that enough power is available to guarantee that the programming voltage is high enough. Before switching on the charge pump, the status of the limiter circuit is checked for about 800µs. When limitation occurs during this time window, the charge pump is activated. After that, the status of the RF limiter is checked continuously by an event counter which evaluates the limiter signals. If the RF voltage drops due to external influence like metal or movement in the field, a certain counter value is not reached during the programming time. This indicates that programming might be not reliable.

If any of the checks fails, a status information is sent to the reader unit for evaluation and reaction. Also the response message to the reader, containing the status, addresses and data is protected by the CRC to avoid false information.

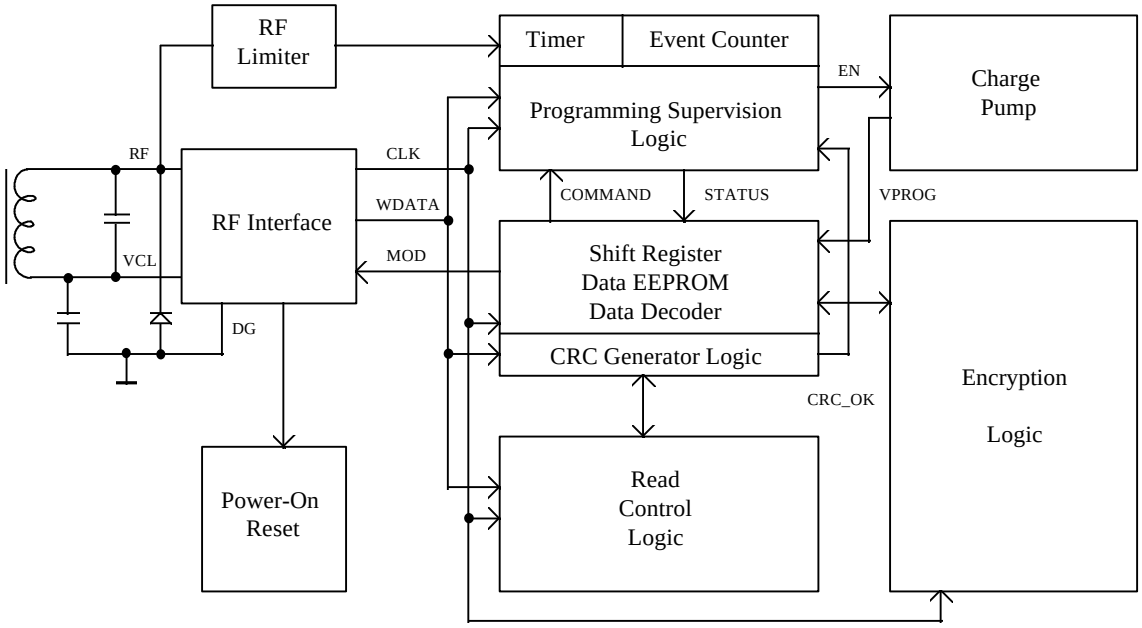

Figure 4: Crypto Transponder Block Diagram

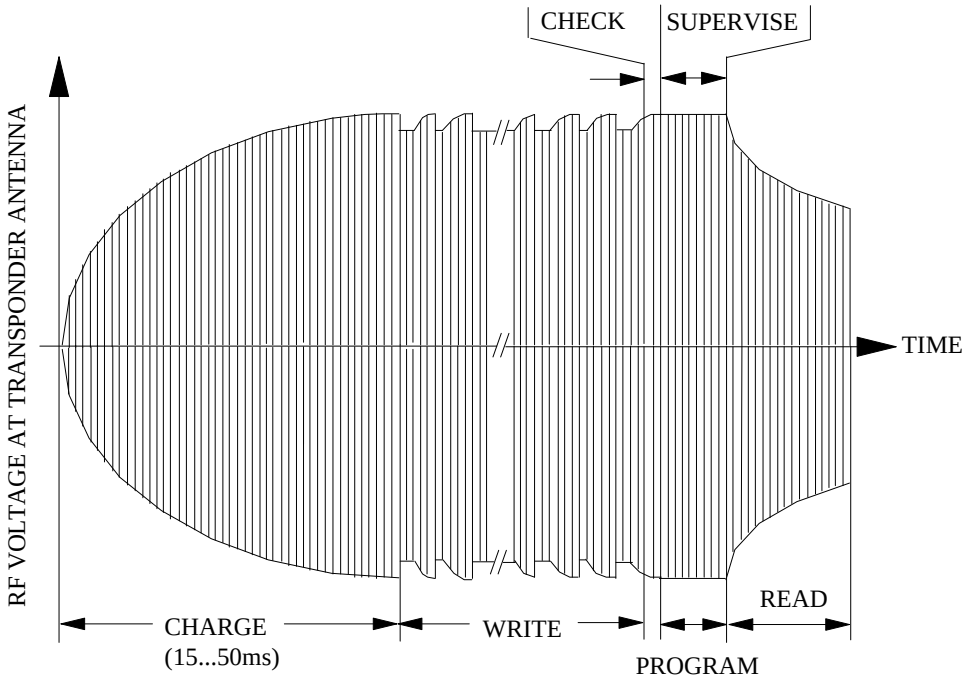

Figure 5: Timing of a Programming Process

7. Summary and Outlook

An overview of various security levels of RFID transponder systems was given. The latest generation technology was presented and some design features described in detail. Compared to standard systems the security level of a crypto transponder is increased significantly. However, constant improvement of the cryptographical algorithms will be necessary in future.

The challenge/response technique however is also well suited for future generation vehicle entry systems, for example Passive Entry. These systems require two way communications. To solve the main issues of Passive Entry, such as faster baud rate, longer ranges, anticollision, the next milestone will be the introduction of a higher, single (or dual) frequency technology which is well suited for the special needs of the automotive market.

http://www.motarway.com mail:motar@371.net