An Open Approach for Designing Secure Electronic Immobilizers

Kerstin Lemke, Ahmad-Reza Sadeghi, and Christian Stüble

Horst Görtz Institute
Ruhr-Universität Bochum
Germany
{lemke, sadeghi, stueble@crypto.rub.de}

Abstract. The automotive industry has developed electronic immobilizers to reduce the number of car thefts since the mid nineties. However, there is not much information on the current solutions in the public domain, and the annual number of stolen cars still causes a significant loss. This generates other costs particularly regarding the increased insurance fees each individual has to pay.

In this paper we present a system model that captures a variety of security aspects concerning electronic immobilizers. We consider generic security and functional requirements for constructing secure electronic immobilizers. The main practical problems and limitations are addressed and we give some design guidance as well as possible solutions.

Keywords: Electronic Immobilizer, Transponder, Motor Control Unit, RFID, Mafia Attack, Distance Bounding, Trusted Computing

1 Introduction

Since the mid nineties, authorities, insurance companies and automotive manufacturers have put much effort in decreasing the number of car thefts in Europe by using electronic immobilizers.[1] An immobilizer system allows the owner of an ignition key to start the car engine. Certainly, improvements have been achieved against car theft through deployment of electronic immobilizers (see, e.g., [16, 1, 12]) but also due to better co-operation between authorities in different countries. However, skilled and determined thieves can still overcome the electronic immobilizer systems ([16]), e.g., through applying advanced attacks such as manipulating the control software of the engine just by using the diagnostic interface.[2] Further, [16] addresses several organizational weak points: the development and production of electronic immobilizers is not sufficiently secured and the trade of diagnostic devices (including the technical details for electronic immobilizers)

[1] For instance Germany is one of the European countries with a high number of stolen cars. This number was 144.057 in 1993 and is reduced to 57.402 in 2002 ([16]).

[2] e.g., around 200 diagnostic devices are currently missing in Germany [4].

cannot be sufficiently controlled due to the annulment of the ‘group exemption ordinance’.

Unfortunately, there is not much technical information about immobilizers publicly available, and details on the current solutions are rarely known, or only some insights are given.[3] As the value loss of stolen cars is large, and this leads to other high costs particularly regarding the additional insurance fees each one of us has to pay, it is worth to reconsider and improve the security of electronic immobilizers.

Based on cryptographic and security measures this contribution aims at providing an “open” approach starting from the functional and security requirements on electronic immobilizer systems down to implementation issues. We point out some practical problems, give design rules and discuss some solutions and open issues concerning electronic immobilizers.

2 System Model

The general model with its components, involved principals, the interfaces between these components and the possible channels to these principals is illustrated in Figure 1. The principals involved are the vehicle manufacturer M, the car owner O, workshops W (approved by the vehicle manufacturer), control authorities A, insurance companies I as well as trusted third parties.

The electronic immobilizer is embedded in the vehicle’s electronics, and consists of three components: The *transponder* T, which is integrated in the *ignition key* of the car, proves its identity towards the *Motor Control Unit* (MCU) that controls the motor engine. The *ignition lock* mainly acts as an interface (e.g., a contactless reader) between transponder and motor control unit, but it can implement some auxiliary functions like a mechanical lock. The communication between the reader and the transponder is radio frequency (RF) based. The transponder obtains its power by the inductive coupling with the RF field that is produced by the reader.

In the following we only briefly consider the involved parties and the trust relations among them. These aspects and the infrastructure required are not the subject of this contribution since our focus concerns the functional and security aspects of electronic immobilizers.

2.1 Trust Relationships

The trust relationships between these parties are very different due to their different interests, and can be very complex. The interests of these parties are manifold: both manufacturers and insurances may tolerate a certain threshold on the number of stolen cars. Beyond this threshold, insurances may react just by adjusting their loss risk, manufacturers may decide to invest into an improved

[3] e.g., by Texas Instruments [12]. Their solution is based on RFID technology and implements a mutual authentication where the underlying cryptographic algorithm used is a proprietary stream cipher.

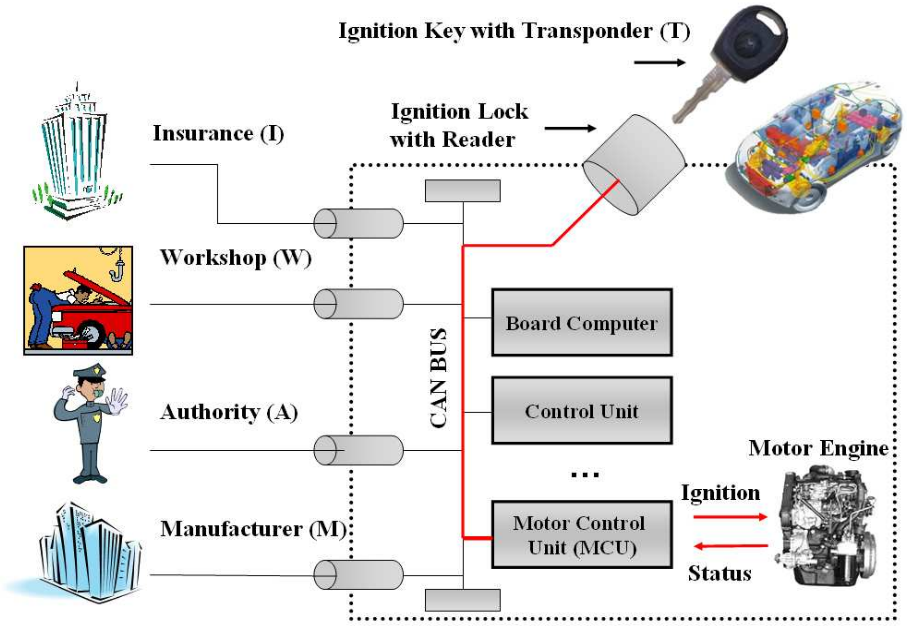

Fig. 1. Infrastructure of the system model.

development of electronic immobilizers to decrease the costs for car insurance or for publicity reasons.

Car owners expect an optimal car theft protection system, including both technical and organizational measures. Car owners and workshops are able to physically access the car components during its operation. One generally assumes that the skills (knowledge and tools) of the workshop employees allow more specific attacks. Manufacturers may be mostly trusted by car owners, while workshops may not. Control authorities are not driven by self-interest and are assumed to play according to the rules to minimize car thefts.

In general, indirect relations (involving a third party) may arise among two principals which lead to more complex relationships. One may consider only two levels of trust, namely full, meaning that a principal is trusted by all other parties, or partial, meaning that this principal is partially trusted by other with respect to certain actions.

The control authority A is the principal who is fully trusted by the other involved principals, but A trusts the other ones only partially. All other trust relations are considered to be only partially.

Primarily, malicious actions are imaginable on behalf of the owner and the workshop. Car thefts can also be made easier because of information leakage at the manufacturer. The car owner is the 'weakest' principal involved who risks to be accused both for the modification of components and/or the co-operation with car thieves. The infrastructure and the corresponding transactions (protocols) should therefore guarantee that an honest owner holds an evidence for having behaved legally. Further relationship exists between subsequent owners of the car. Also here, the trust relationship is considered to be partially.

As mentioned before these aspects have impact on the security of electronic immobilizers, however, they belong to infrastructural and organizational requirements and are not considered further in this contribution.

2.2 Assumptions

Our discussions are based on the following assumptions:

Separation: To keep the system model simple, we assume that the central locking system and the electronic immobilizer are implemented independently, without any interaction, i.e., the corresponding circuits are decoupled.[4]

No Biometrics and no PIN Entry Devices: The ownership of the ignition key is sufficient for the authentication. We do not consider biometric measures or PIN entry devices since (i) they require (costly) security devices and (ii) they do reduce user-friendliness, e.g., if the car owner wants to lend her car to friends.

Organization: Users are responsible for taking care of the ignition keys as well as the corresponding paper documents. The manufacturers provide a key management infrastructure. We further assume that the identifying data and the secret keys involved are already generated and programmed in the non-volatile memory of both the transponder and the motor control unit (e.g., in a secure production environment).

Physical Access: Towing a vehicle cannot be prevented by any electronic immobilizer!

3 Requirement Analysis

A variety of attacks can be mounted for an unauthorized initiation of the ignition process. Possible threats include cloning or simulating transponders[5] or exploiting any weaknesses in the implementation of security mechanisms or when updating the motor control unit and/or the transponder. Moreover, organizational threats against the transponders and the motor control units are of high importance: critical organizational functions concern, e.g., when users order the replacement of transponders or when new motor control units are to be installed (e.g., in workshops). Frauds can also occur during the development and key initialization.

We denote the set of all vehicles with $\mathcal{C}$ and the set of all transponders with $\mathcal{T}$. We call a transponder T *valid*, if there is an approved mapping between $T \in \mathcal{T}$ and the corresponding vehicle $C \in \mathcal{C}$ where the approval is done by a

[4] Nevertheless, there are obviously tendencies to integrate both systems ([2]).

[5] this means being able to construct an device with identical functionality (including the secret initialization data of the target device).

trusted party (such as the manufacturer) or a trusted component certified by this party.[6]

A simple example is a list signed by the trusted party which contains the identification data (ID) of each transponder ID_T and the ID of the vehicle ID_C to which T is assigned by the underlying mapping. We denote the set of valid transponders by $\mathcal{T}_{valid}$. Informally, the main requirements to be fulfilled by an immobilizer system are:

Correctness: A valid transponder $T \in \mathcal{T}_{valid}$ can always invoke the ignition process of the corresponding car.

Security: For a transponder $T^* \notin \mathcal{T}_{valid}$ it shall be infeasible to invoke the ignition process.

To be able to achieve the security objective mentioned above in practice, a variety of technical and organizational building blocks have to be deployed each having own requirements. In the following we will briefly consider these aspects.[7]

3.1 Security Requirements

In this section we consider the generic security requirements most of which are well-known.

Protocol Requirements: Typically, an authentication protocol has to be provided between the transponder and the motor control unit. Security aspects concern protection against active and passive attacks such as eavesdropping the communication between the transponder and the control unit for offline analysis, oracle attacks on the control unit, masquerading and replay attacks, and man in the middle attacks. A type of man in the middle attack is called *mafia fraud* [5] which is of particular concern in the context of wireless systems used for authentication and will be detailed in Section 4.1.

Note that to authenticate the motor control unit, a *mutual authentication* scheme between transponder and motor control unit is reasonable. However, to achieve this in existing vehicles we are faced with the following main problems: Firstly, it is feasible for a skilled adversary to connect a fake MCU to the CAN (Controller Area Network) bus in parallel to the original MCU with the goal to bypass the authentication mechanism later on. To make this hard, the link between MCU and the motor engine has to be separately secured. Secondly, there exists no *trusted path* between the human user and ignition key (e.g., an user interface) yet that can signal to the car owner the result of the authentication (or attestation) protocol.

Evaluation: There should be a possibility to verify the correctness of the applied protocols as specified by the immobilizer specification, e.g., by means

[6] One may desire procedures that do not require trust in manufacturers. However, in practice manufacturers may not be willing to accept this strategy.

[7] Note that the security requirements should remain fulfilled under different implementations, e.g., when software updates of the motor control unit are done by the manufacturer or if test functions are invoked.

of emulators checking the communication on the CAN bus. This would increase the trust of users in the underlying immobilizer systems.

Implementation Requirements: Further, technical requirements concern protection against attacks that exploit implementation weaknesses such as inherent leakage (e.g., side-channel attacks [13, 14]), forced leakage (e.g., fault analysis attacks [6]), and vulnerabilities of the logical or physical construction.

Organizational Requirements: These security requirements concern the life cycle issues, i.e., secure manufacturing, secure initialization (e.g., creation of individual data and cryptographic keys), secure distribution (e.g., transponder maintenance), and secure removal (e.g., destroying of cryptographic keys and components). An important aspect in this context is the requirement that car owners can prove that they are not cheating, e.g., by being able to prove the number of valid transponders even if the car is stolen. Moreover, it should be feasible to detect a complete replacement of the electronic immobilizer system to counteract a typical today's scenario of vehicle theft where a vehicle is first towed to a garage and subsequently the motor control unit is replaced by another one, that was earlier installed in a junk car.

3.2 Usability and Safety Requirements

Next, we list additional requirements of immobilizer systems starting from presumed functional requirements of the automotive industry, caused by safety and usability reasons:

Time Constraints: The execution time of the authentication must be short. This is obvious since the owner is not willing to wait for the engine to start.

Resource Constraints: The resources (e.g., hardware) are constrained. This is more critical for the transponder.

Maintenance: It should be possible to maintain the transponder on behalf of the owner. This includes the cases where the owner wants to block a transponder, e.g., in case it is lost, or add a new one.

Functional Separation: The security functions of the immobilizer should not have impact on safety aspects, e.g., a successful authentication of the transponder should be valid until the motor is turned off (a running motor should not halt for safety reasons).

No Failure Counters: Failed authentication attempts shall not lead to a denial of service.

4 Solutions, Open Issues and Limitations

Based on the requirements of Section 3, we now discuss important aspects to be considered when implementing immobilizer systems.

4.1 Authentication Protocol

Due to the functional requirements on the constrained devices (especially restrictions on the execution time) the use of symmetric cryptography is more efficient than protocols based on asymmetric cryptography.

As mentioned in Section 3.1 the physical link between the motor control unit and the motor engine has to be specially secured. The idea is that an adversary needs more efforts to detach the motor control unit. To make the separation hard for the adversary, a possible solution is to weld the MCU to the engine. However, it is also imaginable that the MCU consists of two parts, one part is hard wired with the engine and the other part is exchangeable.

For the mutual authentication a *trusted path* between the human user and ignition key (e.g., a user interface) that can signal to the car owner the result of the authentication (or attestation) protocol has to be established. Here, a small light-emitting diode on the ignition key might be a solution. Another solution might be the use of the user interface provided by the board computer, however, this implies the assumption that the display cannot be manipulated, which cannot always be guaranteed.

The ISO/IEC 9798-2 three-pass mutual authentication protocol ([3]) using random challenges is proposed as the basic authentication protocol (see also [7]).

Possible cryptographic algorithms for the encryption function include block ciphers, as Triple-DES and AES, and stream ciphers. The cryptographic algorithms Triple-DES and AES are available for direct use, both for encryption and for message authentication codes. A hardware implementation of AES on an RFID based chip is, e.g., presented in [9].

Preventing Mafia Fraud Attacks: Authentication schemes are used in many applications, but as already observed in [5] mafia fraud attacks cannot be prevented *only* by cryptographic mechanisms. The following scenario demonstrates the mafia fraud: consider a car which is parked next to the house of the car owner and the transponder is located inside the house, e.g., near the entrance. A thief gains mechanical access to the ignition lock and inserts a relaying device instead of the ignition key. The relaying device establishes a radio link which is directed towards the owner's house. Once, the transponder is activated by this radio link, the authentication protocol works as specified which leads to a start of the motor engine.

Here, the adversary does not own the transponder, but the adversary establishes a radio link to the transponder. The adversary makes use of the identity of the transponder, without awareness of the car owner.

Preventing the Activation of the Transponder: Mafia fraud attacks are caused by the RF-based activation of the transponder which does not require a human interaction. Therefore, mafia fraud attacks can be blocked if the transponder cannot be activated by the RF field anymore.

One possible solution is to include an ON/OFF switch on the ignition key which allows the car owner to set the transponder in a non-responsive mode. In the non-responsive mode, the transponder does not answer to any requests. Here, the car owner is responsible to care that the transponder is set to a non-responsive mode while not in use. Alternatively, the ignition lock could be used for a mechanical unlocking of the transponder so that the car owner does not need to care about it.

Distance Bounding Protocol: An upper limit on the distance between two physical entities that are involved in a wireless protocol can be determined by precise timing measurements. Electromagnetic waves propagate with the speed of light c, which is approximately $c = 3 \cdot 10^8$ m/s. The spatial extension Δr of an electromagnetic field after a time Δt is given as $\Delta r = c \cdot \Delta t$. A location which is 3 m away from the origin is reached after 10 ns.

As the transponder and motor control unit exchange two messages, two electromagnetic waves propagate in opposite direction. In real life, additional delays have to be considered for the processing in semiconductor devices: at minimum one clock cycle is passed before the answer can be sent back.

In [8] the authors propose distance bounding protocols. The basic idea is as follows: A series of rapid bit exchanges takes place between the involved parties where the number of the bits depends on the security parameter specified. In the corresponding protocol the verifying party V challenges the proving party P, who has access to secret keys, by sending random bits. P has to reply immediately after receiving these bits. The delay time for replies enables V to compute an upper bound on the distance to P. Some precautions should be taken to guarantee that the responses received by V at the bit exchange originally stem from P, e.g., by a prior commitment by P. A modified distance bounding protocol should counteract mafia fraud attacks also in case that the random number generator of the transponder is weak.

The suitability of distance bounding strongly depends on high clock rates at the bit exchange sequence. Automotive immobilizers typically work in the frequency range of 100 kHz ([10]). Using clock frequencies of 100 kHz, it is not worth to implement the Distance Bounding protocol since with the time used for one clock cycle is 10 μs corresponding to a granularity of distance measurements of 3000 m. At frequencies of 13,56 MHz and above, the embedding of Distance Bounding becomes reasonable, at least for hardware based authentication protocols which can minimize the processing delay times.

4.2 Securing the Motor Control Unit

Here, our primary security aim is to prevent the disclosure and modification of secret initialization data of the motor control unit. Further, substitutions of motor control units should be detectable by control authorities later on.

Physical Security: We assume that the core of the motor control unit is a high-performance microcontroller which does not include hardware security mechanisms. In this case, it is recommended to embed the MCU into a tamper-responsive envelope. Note, that 'mal-function' of the MCU is a consequence of tampering if the module is encapsulated. An alternative, but still demanding approach, is the development of a secure 'tamper resistant' high-performance microcontroller.

Since tamper-responsive envelopes are costly, one may be satisfied by using 'only' a small tamper-resistant component that securely stores secrets as long as they are not used. For instance, the *Trusted Platform Module* (TPM) [11] suggested by the trusted computing group[8] (TCG) may be used. The TPM contains an unique certified key, called the endorsement key, that can be used to identify the TPM and thus the motor control unit. Using the TPM, one can also "bind" encrypted content to a specific TPM. This function is called *sealing*, allowing the realization of a secure update function of the control unit software. The *remote attestation* function provided by TPMs allows remote parties to verify the software configuration of the motor control unit using a cryptographically secure hash function. This allows the involved principals to verify the integrity of the installed software of the motor control unit.

Note that an add-on of a TPM requires a secure link between the TPM and each relevant control unit. Further, note that a complete exchange of the TPM and its associated components cannot be prevented either. Nevertheless, the use of a TPM causes higher efforts for the exchange of all associated components. A possible disadvantage might be the complexity that is induced by the TPM.

Interface Security: Attack scenarios as the manipulation of the software with the diagnostic interface are enabled if the design allows to bypass the authentication, either by exploiting flaws or by providing test interfaces which can jeopardize the security of the system. These kinds of attacks can be prevented by a careful system design. Software updates need to be verified by the motor control unit (or by the associated TPM) whether they were originated by the manufacturer before the software is modified. An access to test functions shall only be granted after a successful mutual authentication, e.g., with the valid transponder.

Auditing: As a complete exchange of the motor control unit (which is e.g., swapped out from a wreck of the same type) is hardly to prevent mechanisms should be in place which allow the control authorities to determine whether the MCU was originally fitted in the vehicle or not.

A possible solution is an authentication protocol between the control authority and the MCU that transfers one or multiple unique vehicle identification numbers. With this information either the originality is confirmed or the original place of installation can be revealed. However, note that in practice numbers such as the chassis number can still be manipulated.

4.3 Securing the Transponder

The primary aim is to prevent the disclosure and modification of secret initialization data of the transponder.

Transponders include an IC which is optimized for low power constraints. In [12] it was shown that transponders can include EEPROM memory and use it for the long-term storage of initialization data.

It is obvious that transponders should include security mechanisms to counteract both logical and physical attacks. The complexity of the logical functionality of transponders is quite small so that logical protection is definitively manageable, particularly, software updates are typically not foreseen. Regarding

[8] www.trustedcomputinggroup.org

physical attacks, the transponders should be equipped with passive protection mechanisms to make tamper attempts sufficiently difficult.

4.4 Replacement of Transponders

The ownership of the ignition key shall authorize a principal to start the engine. However, when an ignition key is lost, the owner has to be provided with technical and/or organizational means to block the lost one and obtain and initialize a new one (with new cryptographic keys). There are several solutions imaginable, e.g., those which require a secure channel to the manufacturer or to accredited workshops, and those which do not.

Maintaining Transponders by Infrastructure: In case of an infrastructure maintained by the manufacturer the car owner is provided with a new ignition key if the car owner possesses the original paper documents. The initialization of the ignition key can be done by the manufacturer or at authorized workshops. In the latter case, we assume a secure cryptographic link between the transponder and the initialization center.

Maintaining Transponders by Car Owners: Today, it is very costly for car owners to loose a key because only certified workshops can do the replacement. The possibility for car owners to add new transponders and to remove old (e.g. lost) ones independent of the manufacturer would therefore increase both security and usability. In the following discussion, we are assuming that the non-volatile memory of the transponders can be rewritten and that a symmetric key scheme is used.

We propose a solution where the MCU is the central unit that initializes blank transponders (e.g., ‘duckling principle’ [15]) and that provides appropriate interfaces to authenticate the car owner. As discussed in Section 3, it is essential to ensure that the information how many valid keys currently exist is counted in a secure way, to ensure that owners cannot deceive insurances or buyers of their car. Thus, the MCU cannot be used to store this value, since this information would become unavailable in the case that a car is stolen. Instead, we propose to store the number of valid keys redundantly by all keys. Although this solution requires all transponders to participate this protocol, it has the benefit that the number of valid transponders can be controlled if at least one valid transponder is available.

To prevent that car owners can create secret copies of a transponder, confidentiality of the initialized transponder key has to be guaranteed. One solution is to transmit the cryptographic authentication key in an encrypted form. Therefore, blank transponders have to be shipped with an initial secret key that has to be known by the MCU, requiring some kind of key infrastructure.

Although the proposed solution is on the one hand more flexible and improves the privacy of car owners, it requires on the other hand more complex handling by the car owner. Moreover, the MCU has to provide an interface to perform the authentication of car owners.

But the most important issue is whether the automotive industry is willing to hand over this maintenance function to car owners, since if a manufacturer independent maintenance function is available, the manufacturer and the control authority cannot monitor the personal order of transponders anymore.

4.5 Further Implementation Issues

Random Number Generation: The random number generator should generate an unpredictable sequence of bits (even if the adversary has recorded the previous sequences). A common implementation choice is a pseudo-random generator that is based on a cryptographic cipher and uses two secrets: the key and an initialization value.

Inherent and Forced Leakage: The potential vulnerability of a cryptographic implementation towards inherent and forced leakage cannot be completely assessed by evaluating the design only. Practical tests should be conducted to examine the susceptibility of the implementation to passive and active side channel attacks. Appropriate defenses for the cryptographic implementation include the use of internal random numbers to de-correlate the inherent leakage of the cryptographic device from the secret data processed. Additionally, a de-synchronisation in time is helpful. Fault Analysis can typically be averted by an internal verification of the result to avoid the output of faulty cryptograms. For further details we refer to the various contributions within the side channel related literature. Note, that an encapsulation as suggested in Section 4.2 makes leakage attacks more difficult, as the microcontroller cannot directly be accessed.

4.6 Movement and Positioning Systems

In Section 2.2 it was stated that towing of a vehicle cannot be prevented by an electronic immobilizer. Because of this, adversaries can tow the vehicle to a garage first before they replace components of the vehicle. There already exist sensors (e.g., Hall sensors) which measure the mechanical movement inside the gear of a vehicle. In combination with mobile communication systems (as GSM) alarm events can be signaled to the owner. Additionally, GPS can yield detailed information on the current location of the vehicle. Care should be taken that these sensors cannot easily be detected and disabled or removed before the vehicle is towed.

5 Conclusion

We started an open approach for designing electronic immobilizers. Herein, we presented and discussed a model, the security and functional requirements as well as solution ideas for constructing secure electronic immobilizers. We pointed out some of the main practical problems and limitations when deploying electronic immobilizers and made some suggestions for implementation. Mainly we considered the aspects of the motor control unit and the transponder which is integrated in the ignition key, but we also propose ideas for the key management by the car owner. A complete physical exchange of an electronic immobilizer system cannot be prevented. However, for the future detection of complete exchanges a cryptographic protocol for control purposes should be foreseen.

References

1. http://www.secureyourmotor.gov.uk.
2. http://www.verkehrsunfallforensik.de/pdf/68_Wegfahrsperren.pdf.
3. *ISO/IEC 9798-2: Information Technology – Security Techniques – Entity Authentication – Part 2: Mechanisms using symmetric encipherment algorithms.* International Organisation for Standardization, 1999.
4. Die neue Strategie der Autodiebe. Frankfurter Allgemeine Zeitung, Nr. 40, Seite T1, 2004.
5. Thomas Beth and Yvo Desmedt. Identification Tokens — Or: Solving the Chess Grandmaster Problem. In A.J. Menezes and S.A. Vanstone, editors, *Advances in Cryptology – CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*, pages 169–176. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1991.
6. Eli Biham and Adi Shamir. Differential Fault Analysis of Secret Key Cryptosystems. In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97*, volume 1294 of *LNCS*, pages 513–525. Springer-Verlag, 1997.
7. Colin Boyd and Anish Mathuria. *Protocols for Authentication and Key Establishment.* Springer, 2003.
8. Stefan Brands and David Chaum. Distance-Bounding Protocols. In T. Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1994.
9. Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong Authentication for RFID Systems Using the AES Algorithm. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, volume 3156 of *LNCS*, pages 357–370. Springer-Verlag, 2004.
10. Klaus Finkenzeller. *RFID-Handbook.* Wiley & Sons LTD, 2003.
11. Trusted Computing Group. TPM main specification. http://www.trustedcomputinggroup.org, Nov 2003. Version 1.2.
12. Ulrich Kaiser. Theft Protection by means of Embedded Encryption in RFID Transponders (Immobilizer). ESCAR conference, Cologne, Germany, November 2003.
13. John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Side Channel Cryptanalysis of Product Ciphers. *Journal of Computer Security*, 8(2/3):141–158, 2000.
14. Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. In M. Wiener, editor, *Advances in Cryptology – CRYPTO '99*, volume 1666 of *LNCS*, pages 388–397. Springer-Verlag, 1999.
15. Frank Stajano and Ross Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In *Security Protocols—7th International Workshop*, volume 1796 of *Lecture Notes in Computer Science*, pages 172–194, Cambridge, United Kingdom, 2000. Springer-Verlag, Berlin Germany.
16. W. Thönnes and S. Kruse. Electronical driving authority - how safe is safe? -. VDI Berichte Nr. 1789, 2003.