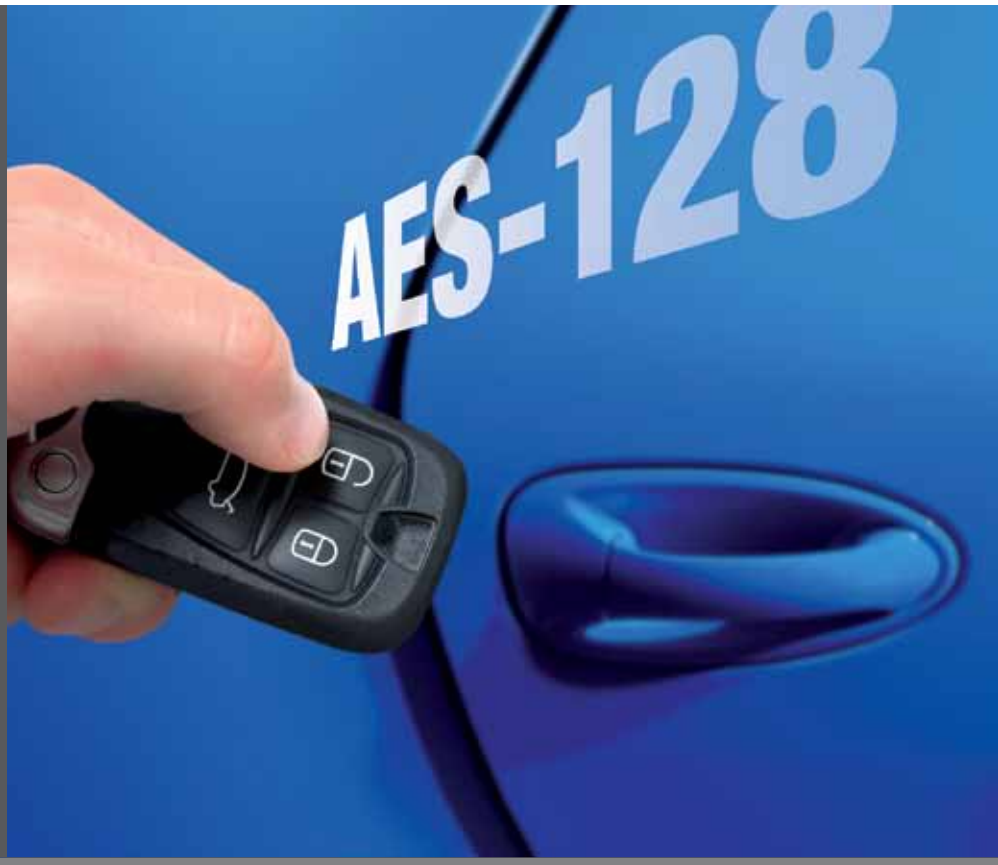
Open Immobilizer System: How Open-source Peer Reviewing Shifts the Security Paradigm

Nicolas Schieli



History

Back in the late 90s, insurance companies made mandatory the implantation of immobilizer devices in all key fobs starting in Germany in January 1998. At that time, immobilizers were read-only RFID transponders carrying simple unique identifiers. In the following years this evolved rapidly into a more complex and secure system embedding cryptographic units and non-volatile memory.

This basic obligation obviously focused IC semiconductor manufacturers on overall system reliability and especially the robustness of the communication link. As with any passive RFID system, immobilizer communication robustness is greatly influenced by the transponder's power consumption. This drove design teams to mainly consider fast cryptographic ciphers (low power) and short communication streams to ease the overall link budget.

In this context, IC semiconductor manufacturers often developed their own cryptography and communication protocol either in-house or through third-party consulting experts with little review by the OEMs. Finally, IC manufacturers started guaranteeing the communication link reliability to the OEMs and Tier suppliers, leading to even more focus on lowering the power consumption and communication duration as much as possible while maximizing the cipher computing efficiency with security level eventually becoming a by-product.

A faulty immobilizer system results in highly visible quality returns at OEMs. Immobilizer systems need to work!

Immobilizer Security Fall-outs

Today, most immobilizer systems based on proprietary cryptography or protocols have documented vulnerabilities that are easily searchable on the Internet. Additionally, some scientists even focused their research field to this specific subject trying to identify conceptual weaknesses in the deployed systems.

One famous example is the scientific publication from the University College London / Université Catholique de Louvain, Belgium titled **Practical Algebraic Attacks on the Hitag2 Stream Cipher**. It demonstrates that the most widely used immobilizer system—Hitag2—is ″extremely week w.r.t. algebraic attacks.″

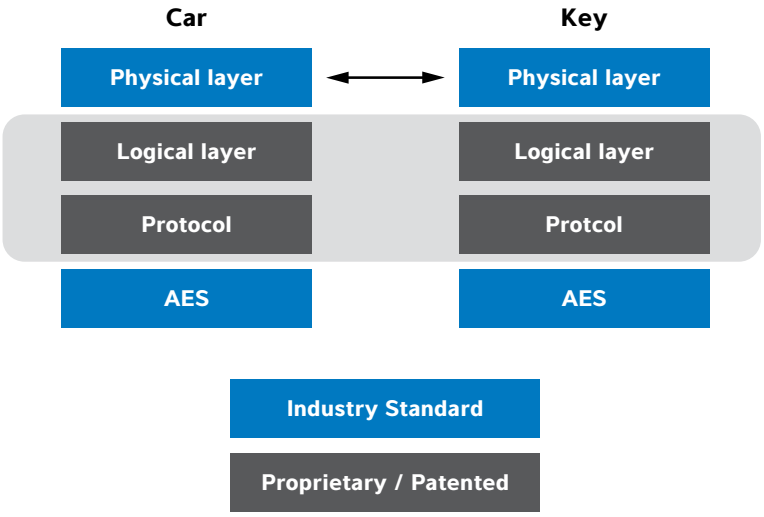


Figure 1. Immobilizer Stack

Besides the obvious security concerns relating to the usage of this technology and the disastrous impact on OEM brands, the more fundamental problem lies with the design methodology that inevitably leads to architecturing vulnerable systems.

Those vulnerable systems relied on the false premise that secrecy would lead to more security. Unfortunately, it consistently leads to the exact opposite outcome.

Ciphers and protocols that remain secret, by definition, see very little peer reviewing during the design phase and get in production with insufficient scrutiny. Thus, the smaller the reviewing team, the higher the risk of unforeseen weaknesses.

"Weak ciphers should be discontinued before they are broken, not after. Trying to keep the specification of insufficiently secure products secret may make things even worse. Then the security of real-life products does collapse very badly one day, when the cipher is reverse engineered" (conclusion of **Practical Algebraic Attacks on the Hitag2 Stream Cipher**).

Due to these growing concerns, the automotive industry is diligently evaluating or even deploying a proven, standardized and open cipher in car access systems: the Advanced Encryption Standard AES-128, which is the result of an international tender of 15 competing ciphers.

AES Alone Does not Solve the Problem

Unfortunately, adoption of the Advanced Encryption Standard in immobilizer systems does not address the whole scope of the security concerns. As depicted in the figure below, the complete stack is divided into 4 layers, the cryptographic unit being only the most advertised one.

In cryptography, a side-channel attack focuses on leveraging weaknesses in the implementation of the cipher or the communication protocol to retrieve the system's secret key without performing a brute force attack (i.e., trying all combinations).

In this context, the protocol layer, if badly designed, could potentially leak out the secret keys or diminish the overall system security unrelated to the intrinsic strength of the AES-128 cipher.

Beyond selecting an intrinsically robust cipher, an immobilizer system security is also a function of:

- Authentication scheme, e.g., unilateral or bilateral
- Communication retry strategies (potentially vulnerable to replay attacks)
- Challenge and response lengths if the complete 128 bits are not transferred (most of the cases for immobilizer systems)
- Hardware protection implemented in the IC against power analysis attack, read out of secret keys from the memory. The newest Atmel® ICs—the ATA5790 and ATA5795—represent the industry's leading edge in hardware protection.

Despite of AES usage in newly designed immobilizer systems, the systems still rely on parameters that are neither

reviewed publicly outside of the IC design team nor have been reviewed by the security community during the IC development phase.

Again, as for the first-generation immobilizers, the security level becomes a by-product of the IC development cycle rather than a broad and continuous peer reviewing process by the whole industry. Bottom line, OEMs have no choice but to use the proposed protocol schemes, hoping that they do not carry security vulnerabilities. As those protocol schemes are often patented or proprietary, OEMs are additionally forced into a single sourcing scheme.

Security as a Design Input Instead of a By-product Result

IC manufacturers will need to continue to guarantee the communication link because reliability remains one of the most important elements of immobilizer systems.

However, within set boundaries, system design trade-offs impacting security at the protocol level should be in the hands of the OEMs instead of isolated IC design teams. This could be achieved with a configurable protocol stack.

Finally, protocol design flaws impacting security should be identifiable early in the design process and ideally fixable through software updates.

This shift in paradigm could be realized at the condition that:

1. The complete immobilizer stack (not only the crypto cipher) is available under an open-source license, thus allowing all parties to scrutinize and enhance the protocols to avoid any security flaws

2. The protocol is configurable to allow the OEMs to select the right trade-offs (security vs. authentication time vs. power budget) with clear boundaries regarding the system reliability

At these conditions security becomes an OEM design input rather than a by-product result..

Atmel Open and Configurable Immobilizer Stack

Open Source Protocol

The Atmel open immobilizer stack is available under an open-source zero-cost license. It has been drafted with the input of security experts, Tier suppliers and OEMs. The protocol is available to the industry as a whole without exception for review, analysis and further enhancement with the end goal of providing the best possible protocol for this specific sensitive application.

Configurable Protocol

As underlined previously, immobilizer systems have competing system requirements:

- Highest security possible
- Fast authentication time
  –The driver shouldn't notice any delay in cranking the engine
- Highest communicate link reliability
  –The immobilizer system is passive and harvests power from the base-station-radiated magnetic field. Lower power systems have better link reliability

The highest possible security, regardless of other system requirements, would need a complete bilateral authentication scheme based on challenge and response of 128 bits each.

The fastest authentication time would require shorter than 128-bit challenges/responses padded with additional internal seeds that can't be random, therefore leading to security limitations.

Lowering the system power (lowering the minimum coupling factor) would require slowing down the AES clock, which directly expands the turn-around time.

What is the Right Security Level?

While each OEM wants to get the highest security possible, they all have different sets of collateral requirements influencing the design trade-offs (minimum coupling factor, maximum authentication time allowed for their system). A one-size-fit all approach can't fit all OEMs.

The Atmel immobilizer stack has configurable options with a subset listed below. Each has a documented impact on authentication time and minimum coupling factor. These parameters are programmed and locked—following customer requirements—by Atmel during manufacturing and cannot be altered once in the field.

The protocol can be audited and customized to OEM needs while Atmel still can guarantee reliable operations.

Parameter	Security Impact	Authentication Time Impact	Minimum Coupling Factor Impact
Unilateral/bilateral authentication	Bit security Strongly depends on challenge length	Strongly depends on protocol type and length of challenge and response	No impact from length of challenge and response but slightly from protocol type
CRC option	No impact	No impact	No impact
Challenge length (32 to 128 bits)	B	~40ms to 140ms for complete authentication cycle	<1.7
Response length (NN to 128 bits)	Bit security: mainly depends on challenge length	See above	See above
AES computation speed	No impact	750µs at 500kHz clock frequency	Lower speed results in slightly lower coupling factor
Encrypted key learning process	No impact	No impact	No impact
2 secret keys instead of 1	Bit security No impact on bit security, but there is an impact on organizational security. Comparable to using a MAC (as in bilateral authentication) that gives limitations in generating random challenges in a scan attack.	No impact	No impact

Bilateral vs. Unilateral

This section briefly describes the procedures implemented to perform unilateral or bilateral authentification with Atmel key-fob circuits.

Replacing "N challenge bits" with 32, and also replacing "M response bits" with 32, results in the fastest configuration for a unilateral authentication protocol.

The most secure configuration possible would require setting "N" as well as "M" to 128 in a bilateral authentication protocol. Certainly, this takes significantly longer than the fast unilateral protocol mainly due to the fact that the number of bits transmitted via the 125-kHz LF field is significantly higher.

Finally, because the protocol is implemented in software, each OEM gets the ability to add or develop its own specific flavor addressing unique use cases.

Open Source Implies Better Quality

An open-source zero-cost license on the protocol helps OEMs better protect their brand against security fall-outs, but also allows multiple sourcing strategies which always implies better quality. An industry-defined protocol excluding lock-in situations help different IC manufacturers providing compatible solutions and focusing on enhancing system performance.

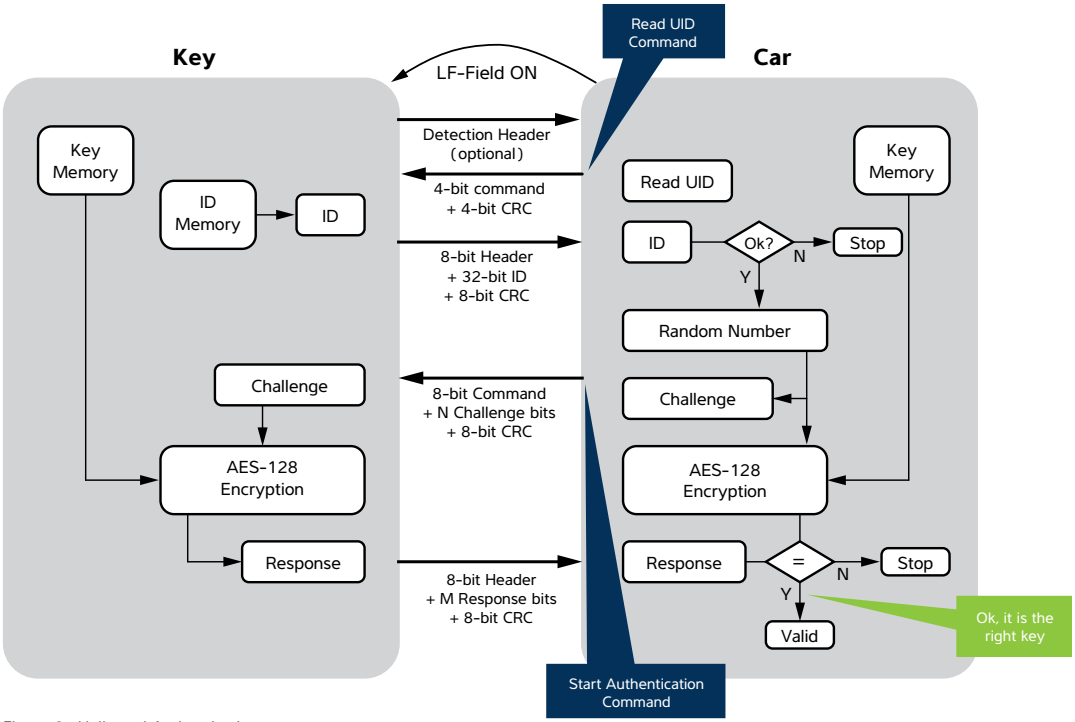


Figure 2. Unilateral Authentication

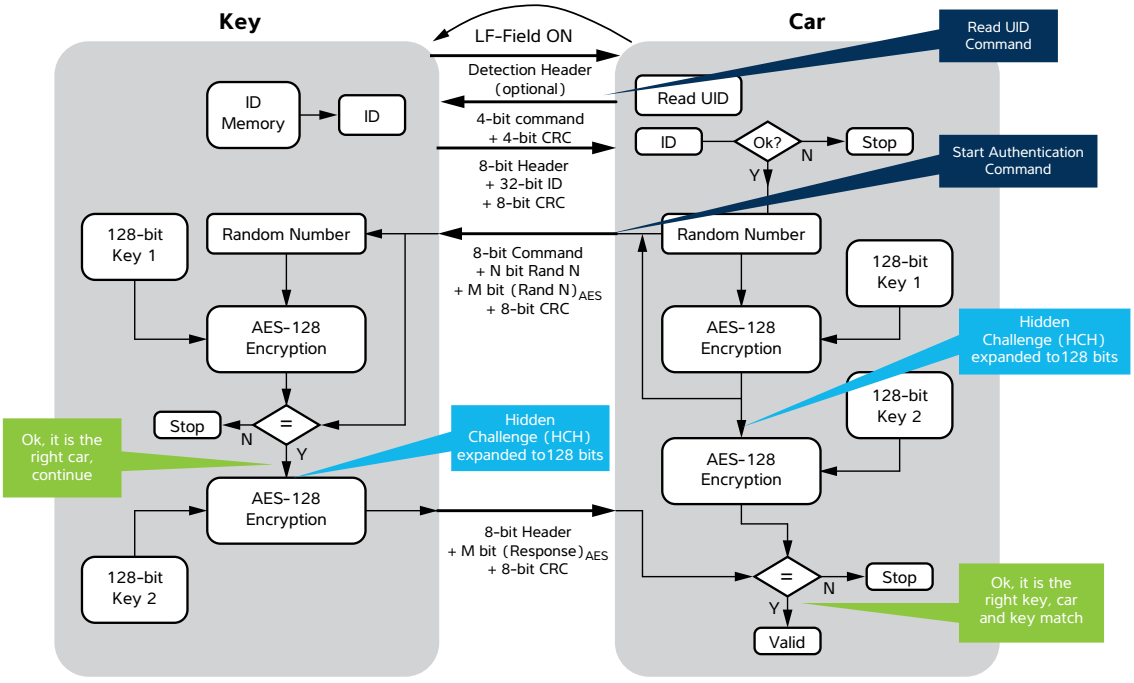


Figure 3. Bilateral Authentication