25th International Scientific Conference UNITECH

International Scientific Conference
20-22 November 2025
GABROVO

ФИЗИЧЕСКИ ПРИНЦИПИ И АНАЛИЗ НА СИГУРНОСТТА НА АВТОМОБИЛНИ ИМОБИЛАЙЗЕР СИСТЕМИ, БАЗИРАНИ НА ТРАНСПОНДЕРИ С МАЛЪК ОБСЕГ

Страхил Събев, Доброслав Данков

Технически университет - Габрово, ул. „Хаджи Димитър“№4, Габрово, България
strahilsubev@gmail.com

PHYSICAL PRINCIPLES AND SECURITY ANALYSIS OF CAR IMMOBILIZER SYSTEMS BASED ON SHORT-RANGE TRANSPONDERS

Strahil Subev, Dobroslav Dankov

Technical University - Gabrovo, 4 Hadji Dimitar St., Gabrovo, Bulgaria
strahilsubev@gmail.com

Abstract
This article presents a comprehensive analysis of short-range automotive immobilizer systems using low-frequency (LF) transponder technology operating at 125 kHz. The basic electromagnetic principles governing the inductive coupling between the transponder and the antenna are presented, the factors determining the effective operating range are analyzed, and current security vulnerabilities and strategies for their prevention are evaluated. The study includes mathematical modeling of electromagnetic interactions, range optimization techniques, and security assessment of modern cryptographic implementations, including AES-128, Hitag, and Megamos protocols. The analysis shows that although LF-based systems provide inherent resistance to remote attacks due to their limited range (2-10 cm), they remain vulnerable to side-channel attacks, relay attacks, and cryptographic weaknesses. Improved security measures are proposed, including dynamic key rolling, hardware-based protection mechanisms, and secure communication protocols to address the identified vulnerabilities.
Keywords: Transponder, crypto, AES, Hitag, immobilizer

ВЪВЕДЕНИЕ

Автомобилният имобилайзър е критична система за сигурност, която предотвратява неоторизираното стартиране на двигателя, освен ако не бъде разпознат валиден електронен ключ. Първо въведени в края на 80-те години, тези системи използват пасивни транспондери, вградени в ключовете на автомобилите, работещи чрез индуктивна връзка с антенни пръстени, позиционирани около цилиндъра на запалването [1,2].

Основният принцип се базира на нискочестотна (LF) електромагнитна комуникация на 125 kHz между антената на автомобила и транспондера. Тази технология се е развила значително, включвайки усъвършенствани криптографски протоколи за противодействие на все по-софистицирани методи на атака. Съвременните реализации използват AES-128 криптиране, превъртащи се кодове и многофакторна автентификация за подобряване на сигурността [3,4].

Print ISSN: 1313-230X, Online ISSN: 3033-1404

ИЗЛОЖЕНИЕ

Системата LF имобилайзер се състои от три основни компонента: антенен пръстен: бобина от меден проводник с 20-100 навивки, работеща на 125 kHz, позиционирана около ключалката за запалването; транспондер: пасивен RFID чип, интегриран в ключа, съдържащ уникална идентификация и криптографски възможности, който получава енергия чрез индукция от антената; контролен блок на имобилайзера (ICU): управлява протоколите за автентификация и комуникира с блока за управление на двигателя (ECU).

Системата работи чрез протокол за автентификация тип «запитване-отговор». Антената генерира носещ сигнал от 125 kHz. Транспондерът събира енергия и отговаря с идентификационни данни. ICU валидира отговора чрез криптографска верификация. При успешна автентификация се дава разрешение за стартиране на двигателя.

При активиране на запалването антената генерира променливо магнитно поле с ниска честота (обикновено 125 kHz). Това поле индуцира напрежение в намотката на транспондера според закона на Фарадей [4]:

$$\varepsilon = -N\frac{d\Phi}{dt} \quad (1)$$

където: ε = индуцирана ЕДН (V); N - брой навивки в бобината на транспондера; Ф - магнитен поток (Wb); A - ефективна площ на бобината (m²); B - плътност на магнитния поток (T).

Получената енергия се използва за захранване на чипа, който изпраща обратно модифициран сигнал чрез промяна на натоварването на антената (load modulation)

Обсегът на индуктивната връзка r е ограничен и зависи от следните параметри: честота на предаване f; радиус на антената a; индуктивност и качествен фактор Q; мощност на предаване Pt; Геометрия на антената и нейното разположение. Приблизителният обсег може да се определи от израза [4]:

$$r = \sqrt[3]{\frac{Pt.Qt.Qr}{R_{eq}.(4\pi f \mu 0)^2}} \quad (2)$$

където: Qt, Qr – качествени фактори на предавателя и приемника, Req – еквивалентно активно съпротивление на веригата, μ_0 магнитна проницаемост на вакуума. На практика, при 125 kHz системи, обсегът е между 2 и 10 cm, в зависимост от размера на антенния ринг и характеристиките на транспондера.

Индуцираното напрежение в транспондера може да се оцени по формулата:

$$V_{ind} = 2\pi f NAB \quad (3)$$

където: A – площ на намотката, B – магнитна индукция .

Магнитната индукция в точка на разстояние r от антената може да се изчисли с следното уравнение:

$$B_{(r)} = \frac{\mu_0 N I a^2}{2(a^2 + r^2)^{3/2}} \quad (4)$$

Тази зависимост показва, че силата на магнитното поле намалява с куба на разстоянието:

$$B \sim \frac{1}{r^3} \quad (5)$$

Затова системите от този тип имат малък обсег и са устойчиви на дистанционни атаки. Честотата от 125 kHz осигурява оптимален баланс между: достатъчно проникване през материали; разумни ограничения на размера на антената; минимални смущения от околни източници; съответствие с международните регулации (ITU-R).

След като транспондерът се захрани, комуникацията между него и антената се осъществява чрез: ASK (Amplitude Shift Keying**)** – модулация чрез промяна на амплитудата; Load modulation – промяна на натоварването на антената за предаване на данни обратно към модула. Типичната скорост на предаване е между 2 и 10 kbit/**s**.

Таблица 1 сравнява различни транспондерни технологии.

Таблица 1

Параметър	LF Транс-пондер (125 kHz)	RF Система (433 MHz)	UHF/BLE (2.4 GHz)
Обхват	2-10 cm	1-30 m	1-100 m
Енергопот-ребление	Ултра-ниско (пасивно)	Ниско-Средно	Средно-Високо
Ниво на си-гурност	Високо (близост)	Средно	Промен-ливо
Чувствител-ност	Ниска	Средна	Висока

Съвременните имобилайзър системи използват няколко криптографски подхода:

Hitag: Hitag1: 32-битов ключ, уязвим на груба сила [5]; Hitag2: собствен поточен шифър, криптографски компрометиран [6]; Hitag Pro (Crypto 3): базиран на AES-128, в момента сигурен [8].

Megamos Crypto: собствен 96-битов шифър; уязвим на диференциална криптоанализа [9]; заменен от aes реализации.

AES-128 системи: индустриален стандарт за криптиране [10]; сигурен при правилна реализация; изисква внимателно управление на ключовете.

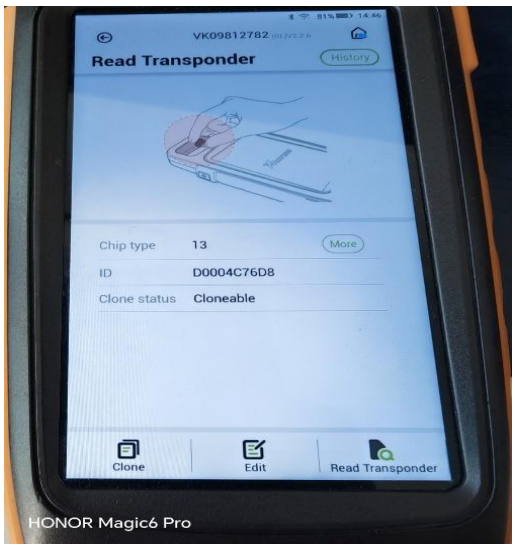
Развитието на транспондерите започва като чипове за съхранение на кода за запалване на автомобила. След време това се оказва съвсем недостатъчно и започват да се интегрират системи с „търкалящ“ код и транспондери с криптирани данни и комуникация. След това са интегрирани в интегрални схеми или процесори и антената е запоена на платката. Така процесорът играе роля на транспондер, дистанционно и други функции в модерният автомобилен ключ.

Съвременните системи като Texas Instruments TMS3705 [1], Philips PCF7936/7946/795x [8], Megamos Crypto48/49 [9] използват 125 kHz енергийна връзка и 134 kHz комуникационен канал с криптографски алгоритми като AES или Crypto-2.

Методи за въздействие и преодоляване на тези защити и възможни противодействия

Методите описани по-долу са от практиката на авторите при ремонт на различните автомобили с проблеми в имобилайзерите.

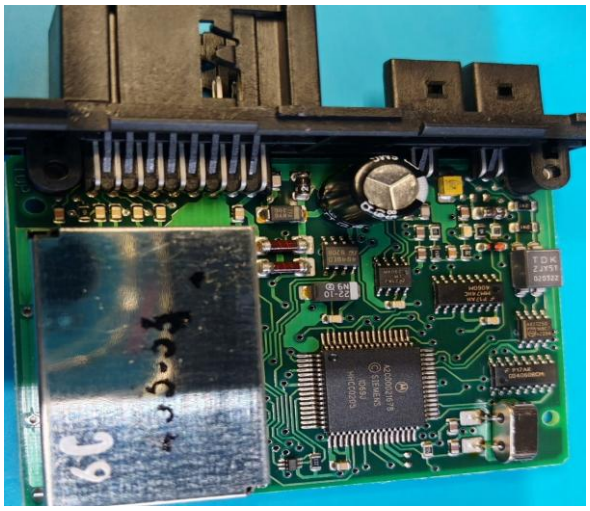
Първите системи от началото на 90-те имат основна слабост и тя е че са много лесни за копиране поради незащитеният от пълно прочитане код в тях. Кодът се прочита и се прави абсолютно копие на транспондера. След това към края на 90 - те започват да се интегрират транспондерите с криптирани данни. Megamos Crypto 48 е изключително масово използван в много автомобили е ясен пример за този подход. Следват интегрираните в процесори на платки Hitag PCF79xx процесори използвани дори до ден днешен. Първите чипове които не са криптирани и не са с „търкалящ“ код са много податливи на атаки и копиране. Копирането им не изисква сложна техника и изчисления.



Фиг.1 *Клониране на чип от старо поколение с ключарска техника. D е въпросният фиксиран код и идентификация на чипа, която трябва да се копира.*

При тези системи противодействие и подобрение е трудно и единствената опция остава минаване на по-сигурна система. Ако липсват ключовете при старите системи това усложнява нещата и

единственият начин за стартиране остава или прочитане на данните от чипа на имобилайзъра или спирането му в двигателният компютър. При някой двигателни компютри това е много трудно или невъзможно. Изчитането на чиповете на някой имобилайзъри също може да е трудоемка задача когато паметта е интегрирана в процесор. На фиг.2 е представен типичен представител на това поколение имобилайзъри, препрограмирането на който е направено от авторите с помощта на апаратурата от фиг.1. Въпросният имобилайзър от Мерцедес е от новото поколение с „търкалящ“ код и криптиран. Края на 90-те започват да се интегрират криптираните транспондери и системи с криптирани чипове с „търкалящ“ код.



Фиг.2 *Имобилайзер на Мерцедес А класа W168 от края на 90-те. Използва Моторола процесор с 64 извода, който трябва да бъде разпоен и прочетен с програматор (практически експеримент, извършен от авторите).*

Разработва се система, която се вгражда в по-скъпите европейски автомобили. За тази система и до ден днешен няма решение как да се копира чипа и да работи повече от един път и да спре и то с риск да увреди вече работещият ключ. До процесорът, в който се съхраняват данните за ключовете в имобилайзъра, няма достъп през диагностичната букса и инсталацията. Единственият начин е процесорът да бъде свален и прочетен през определени точки на интегралната схема. Това прави системата много сигурна и добре подсигурена.

Уязвимости в Megamos Crypto 48.

Алгоритъмът Megamos Crypto използва 96-битов криптографски ключ, но реално ефективната му ентропия е значително по-ниска поради слабости в реализацията и възможността за офлайн криптоанализ. Изследванията на университета Radboud (Нидерландия) [12] показват, че чрез прихващане на няколко интификационни обмена между ключа и блока на имобилайзера е възможно да се възстанови тайната ключова стойност.

Основните проблеми са: липса на достатъчно случайност в предаваните разсейващи стойности; уязвимост към brute-force атаки с предварително изчислени таблици; липса на защита от многократно запитване (anti-replay).

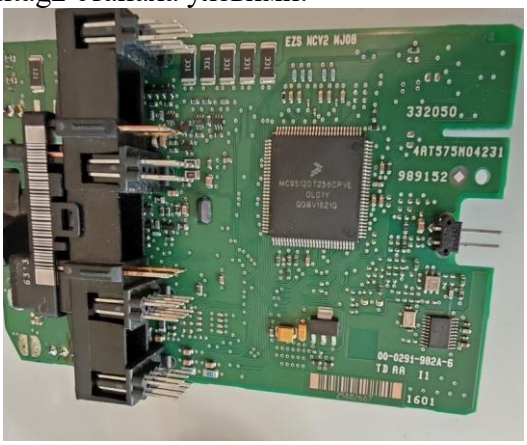
Уязвимости в Philips Crypto (Hitag2)

Системите Philips Crypto II (Hitag2) използват „търкалящ“ код и 48-битов ключ, което днес е крайно недостатъчно ниво на защита. Основните уязвимости включват [7]: криптоанализ на поточния шифър, позволяващ възстановяване на ключа с няколко стотици обмена; слаба обратна връзка в алгоритъма LFSR, което улеснява предсказване на следващи кодове; Replay атаки, при които стар запис на обмен може да бъде използван за стартиране на автомобила.

Методи за подобряване на сигурността. За минимизиране на риска от копиране и клониране на ключове е необходимо прилагане на съвременни криптографски и архитектурни решения: преминаване към AES- или ECC-базирани алгоритми (както при Megamos AES и Hitag AES); използване на подълги ключове (минимум 128 бита) и динамично генерирани случайни nonce стойности; ограничаване на броя на удостоверителни опити – предотвратява офлайн анализ; двуфакторна автентикация между транспондера и блока за уп-

равление – например чрез време-зависим компонент; софтуерни актуализации на имобилайзера и адаптация към нови протоколи и защита и криптиране на комуникационните канали към иммобилайзерният блок за управление.

Транспондери от последно поколение. С напредването на технологиите и развитието на хакерските методи, класическите решения като Megamos 48 и Hitag2 станаха уязвими.



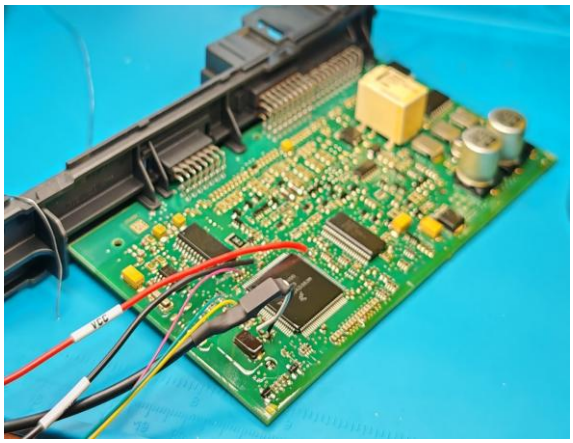
Фиг.3 *Разглобена електронна ключалка на Мерцедес Вито с транспондер последно поколение (заснета от авторите при експериментално препрограмиране).*

В отговор, производителите разработиха ново поколение имобилайзери, базирани на съвременни криптографски алгоритми като AES (Advanced Encryption Standard). Модерните транспондери от този тип -Hitag Pro (Crypto 3), Megamos AES и Texas Crypto AES - вече използват 128-битови ключове, подобрена синхронизация, защита срещу анализ и механизми за ограничаване на опитите за автентикация.

Преглед на съвременните криптографски системи

Технологията Philips Hitag Pro [11] (известна и като Crypto 3) е наследник на Hitag2 и Hitag AES Lite. Тя използва 128-битов AES алгоритъм и динамичен обмен на ключове при всяка автентикация. Основните и характеристики са: Поддръжка на Challenge-Response протокол с времеви разсейващи стойности; Защита срещу повтарящи се атаки чрез еднократно използваеми кодове; Възможност за конфигуриране на нива на сигурност; Вградена логика за ограничение на броя грешни опити, предотвратяваща brute-force атаки.

Системата Megamos AES [13] представлява еволюция на предходния Megamos Crypto 48. Новата версия използва 128-битов AES алгоритъм, включва обратна автентикация и подобрена синхронизация между ключа и имобилайзера. Предимствата и са: невъзможност за извличане на криптографския ключ чрез пасивно подслушване; прилагане на двупосочен отговор с предизвикателство с уникален вектор за инициализация; вградена времева защита срещу странични канали (side-channel attacks) и DPA (Differential Power Analysis).



Фиг.4 *Четене с програматор от интегралната схема на криптиран процесор от имобилайзер на BMW CAS4 използван в F шаситата. Въпросният иммобилайзер използва ключ с Hitag Pro технология (успешен експеримент извършен от авторите).*

Решенията на Texas Instruments (TI DST AES) се използват основно в системи за достъп и стартиране при Ford, Toyota и General Motors. Основни особености са: използване на AES-128 с вътрешен генератор на случайни числа (TRNG); поддръжка на ISO/IEC 18000-3 комуникационен стандарт за LF обхват (125 kHz); устойчивост на fault injection и времеви атаки; възможност за криптографско обновяване на ключовете при сервизен достъп.

Въпреки високото ниво на защита, дори AES-базираните системи не са напълно неуязвими. Основните заплахи са: атаки чрез странични канали (Side-Channel Attacks) – измерване на консумацията на ток или електромагнитни излъчвания при криптографски операции; Fault Injection – инжектиране на смущения в комуникацията или напрежението за извличане на ключови данни; специализирани атаки и достъп до диагностични интерфейси (OBD-II, UDS) – използване на сервизни устройства за нелегално обучение на ключове или ъпдейт с цел извличане на криптирани данни; недостатъчна изолация между модули – някои реализации не защитават адекватно обмена между имобилайзер и ECU.

За ефективно противодействие на горните уязвимости се прилагат следните решения: хардуерна защита срещу странични канали – използване на шумови маскиращи схеми и стабилизирани токови профили; криптографско разделяне на ключовете – съхранение на различни части от ключа в отделни зони на паметта; Dynamic Key Rolling – периодична промяна на основния ключ чрез защитен алгоритъм при всяко стартиране; Secure Boot и криптирани обновления – предотвратяват модификация на софтуера на имобилайзера; усъвършенствана CAN/UDS комуникация – с използване на Message Authentication Codes (MAC) за удостоверяване на всяко съобщение. Модерните имобилайзери, базирани на Philips Crypto 3, Megamos AES и Texas Crypto AES, представляват значителна стъпка напред в сигурността на автомобилните системи. Въпреки това, пълната защита изисква не само силна криптография, но и цялостен подход, включващ хардуерна защита, контрол на достъпа до диагностичните интерфейси и редовни софтуерни актуализации.

Интегрирането на AES-128, комбинирано с анти-смущаващи технологии и динамично управление на ключовете, гарантира надеждност, съответстваща на съвременните изисквания за автомобилна киберсигурност.

ЗАКЛЮЧЕНИЕ

Системите с малък обсег (транспондер и антена) представляват надеждно и енергийно ефективно решение за идентификация в автомобилните имобилайзери. Бъдещите тенденции включват комбиниране на LF идентификация с криптографски алгоритми и допълнителни UHF или BLE канали за гъвкавост при безключов достъп. Модерните имобилайзери, базирани на Philips Crypto 3, Megamos AES и Texas Crypto AES, представляват значителна стъпка напред в сигурността на автомобилните системи. Въпреки това, пълната защита изисква не само силна криптография, но и цялостен подход, включващ хардуерна защита, контрол на достъпа до диагностичните интерфейси и редовни софтуерни актуализации. Интегрирането на AES-128, комбинирано с анти смущаващи технологии и динамично управление на ключовете, гарантира надеждност, съответстваща на съвременните изисквания за автомобилна киберсигурност.

Благодарности: Авторите изразяват своята благодарност за полезните съвети и предложения към всички рецензенти и организатори за подобряване на представянето на проведеното изследване.

Това изследване е финансирано от Европейския фонд за регионално развитие по Оперативна програма „Научни изследвания, иновации и цифровизация за интелигентна трансформация 2021-2027“, проект CoC „Интелигентни мехатронни, екологични и енергоспестяващи системи и технологии“, BG16RFPR002-1.014-0005.

ЛИТЕРАТУРА

[1] Texas Instruments – “RFID Transponder and Reader Systems at 125 kHz”, Application Report (SLAA037).

[2] Philips Semiconductors – “Hitag and Crypto Transponder System Overview”, 2004.
[3] ISO/IEC 11784/85 – “Identification of Animals using LF RFID Systems”.
[4] Finkenzeller, K. – “RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification”, Wiley, 2010.
[5] Volkswagen AG – “Immobilizer IMMO II/III/IV Technical Training Manuals”, 2001–2016.
[6] Garcia, F. D. et al. Lock It and Still Lose It — On the (In)Security of Automotive Remote Keyless Entry Systems, USENIX Security Symposium, 2016.
[7] Verdult, R., Garcia, F., & Balasch, J. Gone in 360 Seconds: Hijacking with Hitag2, USENIX Security Symposium, 2012.
[8] Megamos Crypto Security Analysis – Radboud University Nijmegen Technical Report, 2013.
[9] ISO/IEC 18000-3: Information Technology – Radio Frequency Identification for Item Management.
[10] Garcia, F. D., Oswald, D., et al. Lock It and Still Lose It — On the (In)Security of Automotive Immobilizers, USENIX Security Symposium, 2015.
[11] Philips Semiconductors: Hitag Pro (Crypto 3) Transponder Family — Technical Overview, NXP Technical Documentation, 2022.
[12] Texas Instruments: DST AES Transponder Application Report, TI Security Division, 2021.
[13] Megamos Crypto AES — Automotive Security Platform Whitepaper, Continental AG, 2020.