elektroniczne systemy zabezpieczenia samochodów osobowych, , dekompilacja lub dezasemblacja kodu maszynowego, deszyfracja algorytmu, immobilaiser, klonowanie transpondera, magistrala, urządzenia diagnostyczne, urządzenia emulujące, samodzielne urządzenia dopisujące

Henryk KRÓL[1]

ANALIZA MOŻLIWOŚCI NEUTRALIZACJI IMMOBILISERA

Artykuł zawiera wyniki badań możliwości nieuprawnionego użycia samochodu osobowego zabezpieczonego immobiliserem. W artykule wskazano sposoby neutralizacji immobilisera przy użyciu dostępnych urządzeń elektronicznych. Przedstawiono sposoby postępowania przy deszyfracji algorytmu immobilisera. Uzyskane wyniki eksperymentu nieuprawnionej neutralizacji systemu elektronicznego immobilisera dowiodły, że stosowane rozwiązania sprzętowo-programowe nie są doskonałym zabezpieczeniem samochodu przed włamaniem i kradzieżą.

ANALYSIS OF POSSIBILITY OF CAR IMMOBILISER INACTIVATION

Reseach results of possibilities of illegal use of car protected by immobilser are shown in this paper. Methods of neutralisation of car immobiliser by use common electronic devices are directed. Treatment of decription of immobiliser's internal agorithm was shown. Obtained results of unauthorized neutralisation immobiliser's electronic system showed, that curreutly used hardware-software solutions are not perfect protection of a car against burglary or theft.

1. WSTĘP

Wprowadzenie w latach dwudziestych minionego wieku metody taśmowej produkcji spowodowało upowszechnienie pojazdów i obniżenie kosztów ich produkcji. Ze względu na zapotrzebowanie na części zamienne oraz chęć posiadania samochodu, kradzieże zaczęły wzrastać tak szybko, jak liczba samochodów na drogach. Wraz z rozwojem elektroniki pojawiła się możliwość urozmaicenia i rozbudowania zabezpieczeń samochodów przed kradzieżą. Takim nowoczesnym systemem stał się system immobilisera, który został wprowadzony w latach dziewięćdziesiątych do samochodów osobowych. Elektroniczny kluczyk z transponderem[2], puszka immobilisera[3] wyposażona w mikrokontroler, w którym odbywała się weryfikacja danych dotyczących prawidłowości zastosowanego klucza, przez długi czas stanowiła doskonałe zabezpieczenie samochodu.

[1] Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego w Warszawie, Wydział Elektroniki, 00-908 Warszawa, ul gen. Sylwestra Kaliskiego 2, tel.: 683 92 07, e-mail: *hkrol@wat.edu.pl*
[2] *Transponder* – bezprzewodowy nadawczo-odbiorczy układ elektroniczny z wbudowaną pamięcią.
[3] *Immobiliser* – elektroniczne zabezpieczenie samochodu przed kradzieżą uniemożliwiające jego rozruch.

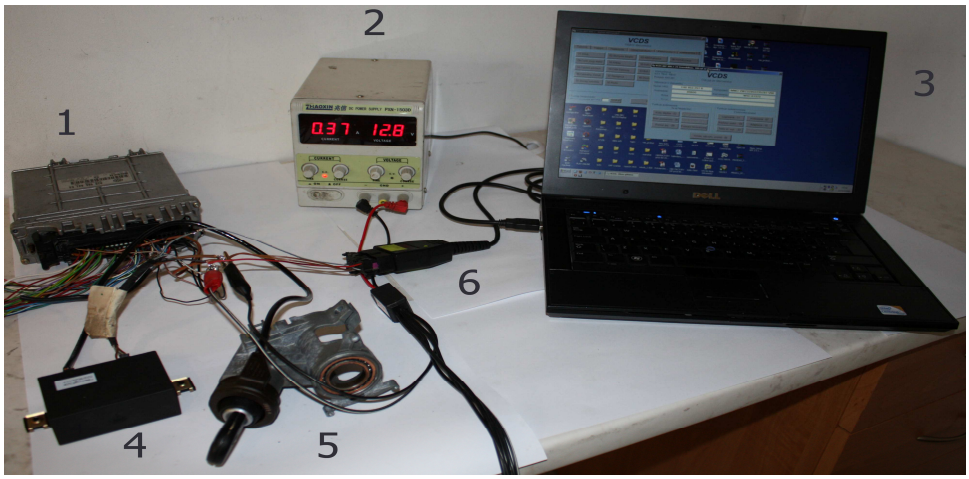
2. SPOSOBY NEUTRALIZACJI IMMOBILISERA

2.1 Wymiana elementów składowych immobilisera

Metoda polega na wymianie elementów elektronicznego zabezpieczenia samochodu przed kradzieżą na już wcześniej zsynchronizowane elementy prawidłowo działającego systemu. Wymianie podlega elektroniczny układ sterujący immobiliserem, elektroniczna jednostka sterująca oraz transponder. Rozwiązanie tego typu jest najmniej skuteczne z perspektywy wymaganego czasu na dokonanie kradzieży. Wynika to z ulokowania elementów elektronicznych zabezpieczenia samochodu przed kradzieżą w różnych, trudno dostępnych miejscach. Elektroniczna jednostka sterująca najczęściej znajduję się pod pokrywą silnika, natomiast elektroniczny układ sterujący immobiliserem umiejscowiony jest wewnątrz samochodu. Potencjalny złodziej poza zsynchronizowanym zestawem musi być wyposażony w szereg narzędzi niezbędnych do dokonania wymiany elementów elektronicznych oraz zneutralizowania blokad mechanicznych.

2.2 Dopisywanie nowego kluczyka

Wykorzystuje się w tym celu urządzenie posiadające funkcję odczytania kodu PIN poprzez złącze diagnostyczne za pomocą odpowiednio przygotowanego oprogramowania kompatybilnego z systemem Windows. Przykładem takiego urządzenia jest interfejs USB Vagtacho angielskiej firmy Automovie ECU Ltd.



Rys 1. Układ badawczy elektronicznego zabezpieczenia samochodu przed kradzieżą

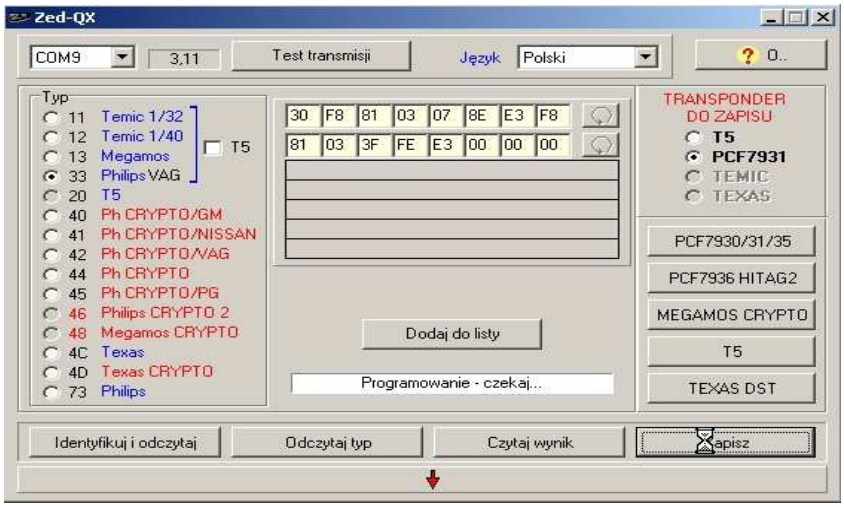
Układ badawczy przedstawiony na rysunku 1 zbudowany jest z:

- elektronicznej jednostki sterującej (ECU) (1);
- zasilacza laboratoryjnego (2);
- komputera z oprogramowaniem diagnostycznym (3);
- immo boxu, układu sterującego immobiliserem (4);
- stacyjki z cewką czytającą i kluczykiem (5);
- interfejsu diagnostycznego (VCDS) (6).

Procedura odczytania kodu PIN oraz dopisania nowego kluczyka jest zautomatyzowana.

2.3 Sklonowanie (skopiowanie) transpondera

Jedną z funkcji urządzenia Zed-QX jest możliwość klonowania transponderów. Klonowanie w tym wypadku polega na odczytaniu pamięci elektronicznej transpondera, który dopisany jest do elektronicznej jednostki sterującej immobiliserem i następnie skopiowaniu zawartości tej pamięci na nowy transponder. Urządzenie posiada możliwość zapisania danych odczytanych z pamięci elektronicznej transpondera w pliku i ich późniejsze odtworzenie. Urządzenie Zed-OX może pracować samodzielnie lub może być sterowane oprogramowaniem z komputera PC poprzez port RS232. Procedura sklonowania (skopiowania) transpondera jest w pełni zautomatyzowana. Charakteryzuję się dużą szybkością działania oraz łatwością w obsłudze.



Rys 2. Okno główne programu do obsługi urządzenia Zed-QX, zapisywanie zawartości pamięci elektronicznej nowego transpondera

2.4 Użycie samodzielnego urządzenia dopisującego

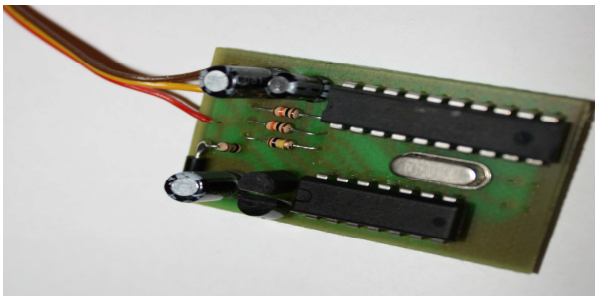
Urządzenie jest oparte na mikrokontrolerze w którym zaimplementowany jest program zawierający procedury oraz inne elementy niezbędne do wykonania określonej, wcześniej wybranej poprzez przyciski konfiguracyjne operacji w samochodzie osobowym. Dodatkowo wyposażone jest w przetworniki pozwalające na wysyłanie i odbieranie komunikatów w standardzie linii diagnostycznej K-Line. Zawiera również diodę informującą o statusie wykonywanej procedury.

Urządzenie posiada szereg funkcji, których wyboru dokonujemy za pomocą przełączników konfiguracyjnych. Za pomocą urządzenia możemy dokonać:

- Dopisania 1, 2, 3 lub 4 kluczyków (transponderów);
- Wyłączenia/Włączenia immobilisera;
- Awaryjnego, jednorazowego wyłączenia immobilisera.

2.5 Urządzenia emulujące prawidłową pracę immobilisera

Urządzenie emulujące elektroniczny układ sterujący immobiliserem jest zintegrowanym układem elektronicznym zbudowanym na bazie mikrokontrolera z zaimplementowanym oprogramowaniem. Dodatkowo wyposażone jest w przetworniki pozwalające na wysyłanie i odbieranie komunikatów w standardzie linii diagnostycznej K-Line.



Rys 3. Elektroniczny emulator układu sterującego immobiliserem

Urządzenie emulujące montuje się zamiast elektronicznego układu sterującego immobiliserem. Należy podłączyć trzy przewody, dwa odpowiedzialne za zasilanie (+12 V, GND) oraz trzeci za komunikację (K-line) z elektroniczną jednostką sterującą pracą silnika.

Po prawidłowej weryfikacji transpondera, układ sterujący immobiliserem inicjuje komunikację z ECU w celu wymiany danych i wzajemnej weryfikacji. Emulator działa na zasadzie pominięcia weryfikacji autentyczności tranpondera i w momencie włączenia zasilania rozpoczyna komunikację z elektroniczną jednostką sterującą pracą silnika. Ze względu na to, że posiada on zaimplementowane oprogramowanie, które zawiera algorytmy odpowiedzialne za wygenerowanie prawidłowych odpowiedzi w postaci kodowanego sygnału, następuje odblokowanie możliwości uruchomienia samochodu.

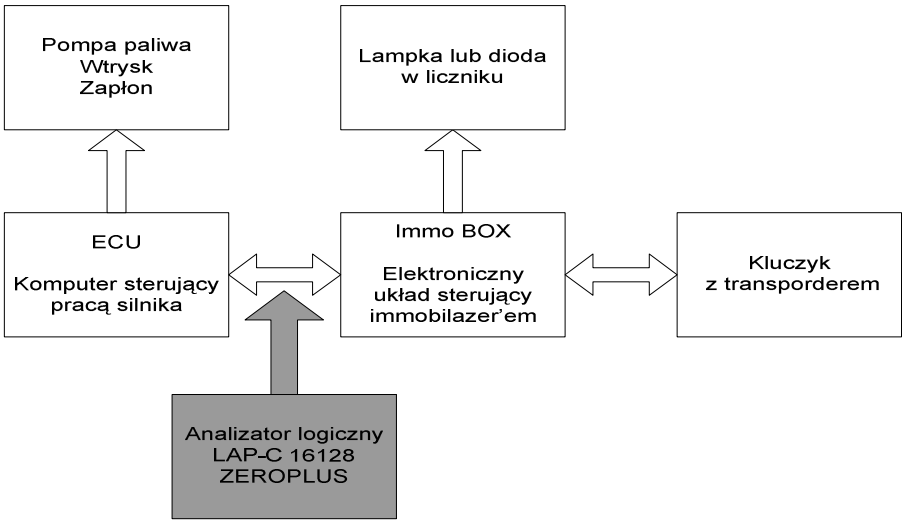
2.6 Dekompilacja lub dezasemblacja kodu maszynowego

Dekompilacja oraz dezasemblacja są metodami polegającymi na zamianie kodu maszynowego (rejestru mikrokontrolera) na kod źródłowy przedstawiony w języku wysokiego bądź niskiego poziomu łatwego w interpretacji dla człowieka. Zamiana kodu maszynowego na język niskiego lub wysokiego poziomu w większości sytuacji jest nie skuteczna ze względu na to, że programy analizujące kod maszynową nie rozróżniają danych od instrukcji. Po konwersji kod zrozumiały dla człowieka jest w szczególności dłuższy od rzeczywistego. Ze względów bezpieczeństwa kod jest dodatkowo zabezpieczany przed dekompilacją i dezasemblacją fałszywymi funkcjami zastosowanymi w programie, które w znaczący sposób utrudniają interpretację. Dodatkowym utrudnieniem jest odczytanie kodów maszynowych z mikrokontrolerów, pamięci FLASH czy EEPROM. Wymagane do tego celu są specjalistyczne programatory. Występują również urządzenia pozwalające na odczytywanie i zapisywanie kodu maszynowego z pamięci FLASH i EEPROM poprzez złącze diagnostyczne. Jednak aby dokonać pełnej dekompilacji lub dezasemblacji niezbędne jest przeanalizowanie wszystkich rejestrów mikrokontrolera zarządzającego danym modułem.

3. DESZYFRACJA ALGORYTMU IMMOBILISERA

3.1 Odczytanie danych z magistrali K-Line

W celu przeprowadzenia deszyfracji algorytmu immobilisera odczytano dane znajdujące się w magistrali K-line podczas weryfikacji autentyczności układu immobilisera przez elektroniczną jednostkę sterującą. Układ badawczy jest identyczny jak na rys. 1. Dodatkowo w układ został włączony analizator logiczny (LAP-C 16128 ZEROPLUS), którego zadaniem było zebranie wszystkich niezbędnych danych do analizy.



Rys 4. Schemat blokowy układu badawczego uzupełniony o analizator logiczny.

Charakterystyczną cechą zastosowanego analizatora logicznego jest obsługa protokołu UART, na którym oparta jest magistrala K-Line. Umożliwia to łatwą interpretację danych.

Rys 5. Opis pakietu w oknie roboczym dla magistrali UART

Badania przeprowadzono na dwóch standardowych systemach immobilisera pochodzących z samochodów VW Passat B5 oraz Seat Toledo II.

3.2 Analiza danych z magistrali K-Line

Tabela 3.1 Pakiety wymiany danych między jednostką sterującą a immobiliserem.

	VW Passat B5					***Seat Toledo II***				
Pomiar / Pakiet	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
1	00	00	00	00	00	00	00	00	00	00
2	07	07	07	07	07	07	07	07	07	07
3	F8	F8	F8	F8	F8	F8	F8	F8	F8	F8
4	**01**	**01**	**01**	**01**	**01**	**01**	**01**	**01**	**01**	**01**
5	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE
6	**D7**	**D7**	**D7**	**D7**	**D7**	**D7**	**D7**	**D7**	**D7**	**D7**
7	28	28	28	28	28	28	28	28	28	28
8	***14***	***8A***	***C5***	***E2***	***71***	***3B***	***1D***	***8E***	***C7***	***63***
9	EB	75	3A	1D	8E	C4	E2	71	38	9C
10	***DD***	***6F***	***37***	***9B***	***4D***	***44***	***A2***	***D0***	***68***	***B4***
11	22	90	C8	64	B2	BB	5D	2F	97	4B
12	***DA***	***DA***	***DA***	***DA***	***DA***	***05***	***05***	***05***	***05***	***05***
13	25	25	25	25	25	FA	FA	FA	FA	FA
14	***6F***	***6F***	***6F***	***6E***	***6F***	***DA***	***DB***	***DB***	***DA***	***DA***
15	90	90	90	91	90	25	24	24	25	25
16	03	03	03	03	03	03	03	03	03	03
17	07	07	07	07	07	07	07	07	07	07
18	F8	F8	F8	F8	F8	F8	F8	F8	F8	F8
19	**02**	**02**	**02**	**02**	**02**	**02**	**02**	**02**	**02**	**02**
20	FD	FD	FD	FD	FD	FD	FD	FD	FD	FD
21	**3D**	**3D**	**3D**	**3D**	**3D**	**3D**	**3D**	**3D**	**3D**	**3D**
22	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2
23	***89***	***AC***	***AD***	***A4***	***80***	***80***	***89***	***AD***	***AD***	***84***
24	76	53	52	5B	7F	7F	76	52	52	7B
25	***08***	***04***	***52***	***18***	***4C***	***4E***	***56***	***0A***	***44***	***52***
26	F7	FB	AD	E7	B3	B1	A9	F5	BB	AD
27	***76***	***F6***	***F6***	***F6***	***76***	***01***	***81***	***01***	***01***	***01***
28	89	09	09	09	89	FE	7E	FE	FE	FE
29	***9B***	***9B***	***9B***	***9B***	***9B***	***76***	***76***	***76***	***76***	***76***
30	64	64	64	64	64	89	89	89	89	89
31	03	03	03	03	03	03	03	03	03	03
32	**03**	**03**	**03**	**03**	**03**	**03**	**03**	**03**	**03**	**03**
33	FC	FC	FC	FC	FC	FC	FC	FC	FC	FC
34	**03**	**03**	**03**	**03**	**03**	**03**	**03**	**03**	**03**	**03**
35	FC	FC	FC	FC	FC	FC	FC	FC	FC	FC
36	**09**	**09**	**09**	**09**	**09**	**09**	**09**	**09**	**09**	**09**
37	F6	F6	F6	F6	F6	F6	F6	F6	F6	F6
38	03	03	03	03	03	03	03	03	03	03

Z pomiarów w obu zbadanych systemach wynika, że:

- pakiety **1-7**, **16-22** oraz **31-38** we wszystkich pomiarach mają te same wartości,
- pakiety **8-15** oraz **23-30** we wszystkich pomiarach mają różne wartości,
- odebranie danych potwierdzane jest w magistrali poprzez odesłanie zanegowanych danych (np. **01-FE**, ***DA*-25**, **05-FA**).

Na tej podstawie stwierdzono, że:

- pytania znajdują się w pakietach 8-15,
- odpowiedzi znajdują się w pakietach 23-30.

Dodatkowo z pakietów pytań i odpowiedzi można usunąć zanegowane pytania i odpowiedzi, aby uzyskać większą przejrzystość danych do analizy.

Tabela 3.2 Zestawienie wyodrębnionych pytań i odpowiedzi z uzyskanych pomiarów.

		VW Passat B5					***Seat Toledo II***				
Pomiar / Pakiet		***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
8	A_p	***14***	***8A***	***C5***	***E2***	***71***	***3B***	***1D***	***8E***	***C7***	***63***
10	B_p	***DD***	***6F***	***37***	***9B***	***4D***	***44***	***A2***	***D0***	***68***	***B4***
12	C_p	***DA***	***DA***	***DA***	***DA***	***DA***	***5***	***5***	***5***	***5***	***5***
14	D_p	***6F***	***6F***	***6F***	***6E***	***6F***	***DA***	***DB***	***DB***	***DA***	***DA***
23	A_o	***89***	***AC***	***AD***	***A4***	***80***	***80***	***89***	***AD***	***AD***	***84***
25	B_o	***8***	***4***	***52***	***18***	***4C***	***4E***	***56***	***A***	***44***	***52***
27	C_o	***76***	***F6***	***F6***	***F6***	***76***	***1***	***81***	***1***	***1***	***1***
29	D_o	***9B***	***9B***	***9B***	***9B***	***9B***	***76***	***76***	***76***	***76***	***76***

Z wyników pomiarów przedstawionych w tabeli 3.2 wynika, że układ sterujący immobiliserem otrzymuje cztery pytania: A_p, B_p, C_p oraz D_p (w czterech kolejnych pakietach), następnie na nie odpowiada w postaci czterech pakietów A_o, B_o, C_o oraz D_o (w czterech kolejnych pakietach).

3.2 Rozwiązanie algorytmów odpowiedzi

Do rozwiązania algorytmów odpowiedzi na pytania przyjęto założenia, że procesory w ALU[4] mogę wykonywać podstawowe operacje arytmetyczno-logiczne, generowanie odpowiedzi musi być procesem krótkotrwałym oraz ograniczenia magistrali K-Line takie jak szybkość transmisji 9600 bit/s oraz RxD i TxD na jednej linii.

System immobilisera oparty jest na mikrokontrolerach i procesorach 8-bitowych. Przesyłane dane są w postaci pakietów 8 bitowych. Po przeanalizowaniu wyników z bezpośrednich pomiarów zauważono wspólne cechy łączące pytania C_p oraz D_p z odpowiedziami C_o oraz D_o w obu badanych przypadkach:

- pytania C_p zawsze przyjmują taką samą wartość (VW B5 – DA; Seat Toledo II - 05) - odpowiedzi C_o przyjmują dwie wartości (VW B5 – 76 lub F6; Seat – 01 lub 81)
- pytania D_p zawsze przyjmują dwie wartości (VW B5 –6E lub 6F; Seat – DA lub DB) - odpowiedzi D_o przyjmują jedną wartość (VW Passat B5 – 9B; Seat Toledo II – 76)

[4] *ALU* (*Arithmetic and Logical Unit* or *Arithmetic Logic Unit*) – część procesora odpowiedzialna za wykonywanie prostych operacji arytmetycznych oraz logicznych.

Z przeprowadzonej analizy wynika, że algorytmy generowania odpowiedzi na pytania C_p oraz D_p są zależne od innych zmiennych wejściowych:

- C_p od A_p lub B_p,
- D_p od A_p lub B_p lub C_p.

Tabela 3.3 Zestawienie pytań C_p, D_p oraz odpowiedzi C_o, D_o

VW Passat B5				***Seat Toledo II***			
Pytania		Odpowiedzi		Pytania		Odpowiedzi	
HEX	***BIN***	***HEX***	***BIN***	***HEX***	***BIN***	***HEX***	***BIN***
DA	11011010	76	01110110	5	00000101	01	00000001
6E	01101110	F6	11110110	**DA**	11011010	81	10000001
6F	01101111	**9B**	10011011	**DB**	11011011	**76**	01110110

Na podstawie danych w tabeli 3.3 stwierdzono, że sześć bitów najbardziej znaczących pytania jest zawsze sześcioma bitami najmniej znaczącymi odpowiedzi. Zauważono przesunięcie dwu bitowe w lewo. Odpowiedź D_o generowana jest na podstawie pytań D_p oraz pytania C_p. Obie liczby są traktowane jako dwa bity „ustawione" kolejno:

$C_p D_p = 11011010\ 01101110_2 \rightarrow DA\ 6E_{16}$
$C_p D_p = 11011010\ 01101111_2 \rightarrow DA\ 6F_{16}$
$C_p D_p = 00000101\ 11011010_2 \rightarrow 05\ DA_{16}$
$C_p D_p = 00000101\ 11011011_2 \rightarrow 05\ DB_{16}$

Z kolei dokonywane jest przesunięcie o dwa bity w lewo w celu uzyskania odpowiedzi D_o:

$C_p D_p = XX110110\ 10011011\sout{10}_2 \rightarrow D_o = 9B_{16}$
$C_p D_p = XX110110\ 10011011\sout{11}_2 \rightarrow D_o = 9B_{16}$
$C_p D_p = XX000001\ 01110110\sout{10}_2 \rightarrow D_o = 76_{16}$
$C_p D_p = XX000001\ 01110110\sout{11}_2 \rightarrow D_o = 76_{16}$

Gdzie $X = 0_2$ lub 1_2

Po przesunięciu zmiennych C_pD_p o dwa bity w lewo powstały dwa nowe bity XX na miejscach najbardziej znaczących. Po usunięciu odpowiedzi D_o ze zmiennych C_pD_p pozostałe sześć bitów najmniej znaczących jest sześcioma bitami najmniej znaczącymi odpowiedzi C_o. Ze względu na znaczące podobieństwa między pytaniami i odpowiedziami C, D oraz stwierdzeniu udziału pytania C_p w generowaniu odpowiedzi D_p sprawdzono dwa najmniej znaczące bity pytania B_p i porównano je do dwóch bitów odpowiedzi C_o.

Tabela 3.4 Zestawienie pytań B_p oraz odpowiedzi C_o.

VW Passat B5	***1***	***2***	***3***	***4***	***5***
Pytanie: $\mathbf{B_p}$	11011101	01101111	00110111	10011011	01001101
Odpowiedz: $\mathbf{C_o}$	01110110	11110110	11110110	11110110	01110110
Seat Toledo II	***1***	***2***	***3***	***4***	***5***
Pytanie: $\mathbf{B_p}$	11011010	11011000	01110110	00111010	00011100
Odpowiedz: $\mathbf{C_o}$	10000001	00000001	10000001	10000001	00000001

Z danych w tabeli 3.4 wynika, że dwa najmniej znaczące bity z pytania B_p są przesuwane w prawo i stają się dwoma najbardziej znaczącymi bitami w odpowiedzi C_o. Odpowiedź C_o generowana jest na podstawie pytań C_p oraz pytania B_p. Obie liczby są traktowane jako dwa bity „ustawione" kolejno:

$$B_p\,C_p = 11011101\ 11011010_2 \rightarrow DD\ DA_{16}$$
$$B_p\,C_p = 01101111\ 11011010_2 \rightarrow 6F\ DA_{16}$$
$$B_p\,C_p = 11011010\ 00000101_2 \rightarrow DA\ 05_{16}$$
$$B_p\,C_p = 11101100\ 00000101_2 \rightarrow EC\ 05_{16}$$

Przeanalizowano również możliwe powiązania pytania B_p z innymi pytaniami. Zauważono, że dla parzystych pytań A_p odpowiedzi B_o przyjmują wartości maksymalnie do $1E_{16}$. Natomiast dla nieparzystych pytań A_p odpowiedzi B_o przyjmują wartości maksymalnie $5C_{16.}$ Wynika stąd, że odpowiedź może być maksymalnie liczbą 5 bitową ($1E_{16}=11110_2$) dla pytania A_p parzystego oraz 7 bitową ($5C_{16}=1011100_2$) dla pytania A_p nieparzystego. Zaobserwowano również, że odpowiedzi B_o zawsze są parzyste. Świadczy to o tym, że w algorytmie generującym odpowiedź zastosowano mnożenie razy dwa (przesunięcie bitowe o jeden bit w lewo) w celu uzyskania parzystej liczby.

W celu uzyskania odpowiedzi B_o (5 bitowej) dla pytania A_p parzystego dokonano przesunięcia o trzy bity w prawo 8 bitowego pytania B_p (5 bitów najbardziej znaczących):

$$B_p >> 3 = 11110101_2$$

Wynik pomnożono przez dwa (przesunięto o jeden bit w lewo) aby uzyskać parzystą liczbę:

$$B_p << 1 = 11100_2$$

Następnie zanegowano 4 najbardziej znaczące bity wyniku przesunięcia $B_p << 1$:

$$B_o = 00010_2 \rightarrow B_o = 2_{16}$$

Dla takich samych pytań B_p (np. 92_{16}), ale parzystych i nieparzystych A_p istnieje stała zależność w odpowiedzi B_o. Jest to różnica między odpowiedziami wynosząca $5A_{16}$ - $1A_{16}$ = 40_{16}. Aby uzyskać wynik dla A_p nieparzystego należy do otrzymanego wyniku dodać wartość 40_{16}.

$$B_p >> 3 = 10010010_2$$
$$B_p << 1 = 00100_2$$

Następnie zanegowano 4 najbardziej znaczące bity wyniku przesunięcia $B_p << 1$ i dodano wartość 40_{16}:

$$B_o + 40_{16} = 1011010_2 \rightarrow B_o = 5A_{16}$$

Algorytm uzyskania odpowiedzi B_o oparty jest na przesunięciach bitowych oraz negacji.

W celu sprawdzenia rozwiązania algorytmów generujących odpowiedzi B_o, C_o oraz D_o stworzono specjalny arkusz kalkulacyjny. Arkusz opracowano w środowisku programistycznym Java za pomocą darmowego kompilatora NetBeans IDE 6.9.1.

Do arkusza kalkulacyjnego wprowadza się dane wejściowe w pola Pyt A (A_p), Pyt B (B_p), Pyt C (C_p) oraz Pyt D (D_p). Następnie po kliknięciu w przycisk „Przelicz" otrzymuje się dane wyjściowe w polach Odp A (A_p), Odp B (B_p), Odp C (C_p) oraz Odp D (D_p).

4. WNIOSKI

Współczesna ochrona samochodów osobowych przed kradzieżą to grupa systemów mających na celu maksymalne utrudnienie oraz wydłużenie czasu kradzieży samochodu. Są to systemy mechaniczne w postaci np. blokady kierownicy czy skrzyni biegów, systemy elektromechaniczne (np. centralny zamek, elektroniczna blokada kierownicy), systemy alarmowe oraz systemy monitorowania GPS. Skutecznym zabezpieczeniem przed kradzieżą jest też przechowywanie samochodu w bezpiecznym miejscu (np. parking strzeżony, garaż), które jest zabezpieczone przez własne systemy bezpieczeństwa w formie ochrony fizycznej i technicznej. Przez ponad 100 lat nie udało się konstruktorom skutecznie zabezpieczyć samochodu. Zawsze gdy tworzono pewne zabezpieczenie z czasem złodzieje potrafili je obejść. Można przyjąć, że skutecznym zabezpieczeniem samochodu jest zastosowanie dużej liczby różnych systemów w jednym pojeździe.

Według danych policyjnych zabezpieczenie pojazdu elektronicznym układem immobilisera nie spowodowało znacznego zmniejszenia liczby kradzieży samochodów osobowych, jednak w znaczny sposób utrudniło ten proceder i wydłużyło czas kradzieży. W ramach badań podjęto próbę deszyfracji algorytmu immobilisera dla dwóch wybranych pojazdów wyposażonych w standardowy system elektronicznego zabezpieczenia samochodu przed kradzieżą tego samego typu. Przeprowadzono szereg pomiarów w celu uzyskania niezbędnej liczby danych do analizy. Na tej podstawie uzyskano algorytm deszyfrujący dla danych odpowiedzi. Algorytm zaimplementowano do specjalnie przygotowanego arkusza kalkulacyjnego w środowisku Java. W wyniku przeprowadzonych badań wyciągnięto nstp. wnioski:

- immobiliserowi należy nadać szczególny priorytet podczas konstruowania systemu;
- należy zwiększyć prędkość transmisji danych lub zastosować inną, szybszą magistralę np. dwuliniową magistralę z oddzielnym RX i TX, co pozwoli na przesłanie większej liczby informacji w tym samym czasie;
- w urządzeniach odpowiedzialnych za obsługę algorytmu generującego pytania i odpowiedź należy zastosować szybsze szesnastobitowe procesory;
- algorytm szyfrujący należy w znaczny sposób ulepszyć, aby interpretacja danych nie była możliwa dla małej liczby pomiarów. Można tego dokonać poprzez zwiększenie liczby pytań oraz działań arytmetycznych generujących odpowiedzi.

5. BIBLIOGRAFIA

[1] Drzewiecki P., *Elektrotechnika i elektronika w pojazdach samochodowych*, KaBe, Krosno 2006.
[2] Herner A., Hans-Jurgen R.: *Elektronika i elektronika w pojazdach samochodowych*, WKiŁ, Warszawa 2007.
[3] Nawrocki W.: *Sieci wymiany danych w pojazdach samochodowych*, WKiŁ, Warszawa 2009.
[4] Proniewski M.: *Immobilizery - jakie powinny być ?*, Systemy Alarmowe 6/1997.
[5] Wicher J.: *Bezpieczeństwo samochodów osobowych i ruchu drogowego*, WKiŁ, Warszawa 2004.
[6] Wrzask L.: *Elektrotechnika i elektronika w samochodach*, KaBe, Krosno 2009.
[7] *VAGTACHO USB - User Guide*, Automovie ECU Ltd. 2010.
[8] Zimmermann W., Schmidgall R.: *Magistrale danych w pojazdach*, WKiŁ, Warszawa 2008.