Jak działają piloty radiowe

Kod stały

Wygodni amerykanie, którym nie chciało się wychodzić z auta gdy wracali do domu, wymyślili sterowane pilotem radiowym siłowniki do bram garażowych.

Pilot był konstrukcją adekwatną do ówczesnego stanu elektroniki, mikroprocesory jeszcze nie istniały, był nadajnikiem radiowym, który konfigurowało się przełącznikiem tzw. DIPswitchem 8 -10 lub12 pozycyjnym.

Pilot radiowo przekazuje stan swoich przełączników DIPswitcha poszerzony o stan wciśniętego klawisza, a odbiornik porównuje odebrany stan przełączników DIPswicha pilota, z przełącznikami swojego DIPswicha i jeżeli jest identyczny, reaguje na przesłany wciśnięty klawisz.

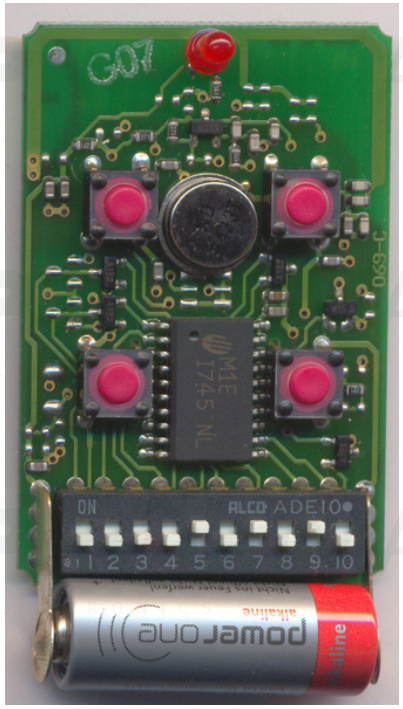
W tym systemie, poprawną pracę zapewniają identycznie ustawione w pilotach i w odbiorniku DIPswitche.

Odbiornik nie posiada pamięci kodu – ponieważ jego pamięcią jest DIPswitch w odbiorniku.

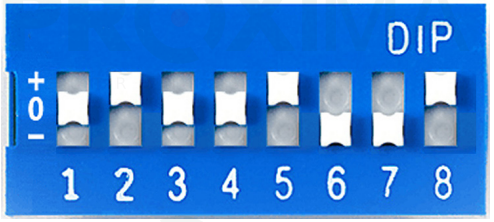
DIPswitche posiadają 8 -10 lub12 przełączników.

Daje to 2^8, lub 2^{10}, lub 2^{12} kombinacji - odpowiednio 256, 1024 lub 4096 kombinacji – czyli bardzo mało.

Takich pilotów używa się do dziś – dobrym przkładem jest NICE FLO o 1024 kombinacjach.



Istnieją też piloty wyposażone w DIPswitche, w których każdy przełącznik można ustawić w trzech, a nie dwóch stabilnych pozycjach.



Zwiększa to ilość kombinacji do 3^8, 3^{10} i 3^{12}, odpowiednio 6561, 59049, 531441 kombinacji.
W systemie tym łatwo jest dorobić pilota – wystarczy kupić pilota i ustawić DIPswitche w nowym pilocie identycznie jak w pilocie działającym.

Ale czas biegł dalej, pojawiły się mikroprocesory i producenci unowocześniając wyroby i chcąc zachować zgodność systemu zastąpili DIPswitche fizyczne – DIPswitchami wirtualnymi.

Ditec na przykład: zamiast ustawiania kodów DIPswitchami fizycznymi, wprowadził ustawiania kodów przyciskami pilota (dziesięciopozycyjny wirtualny DIPswitch).

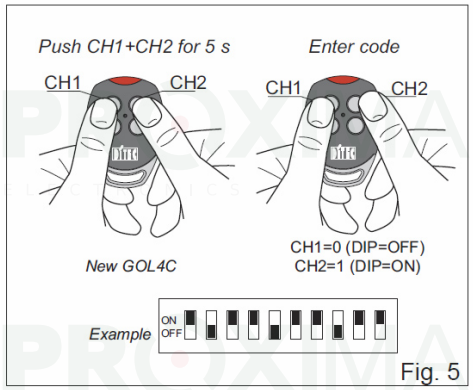
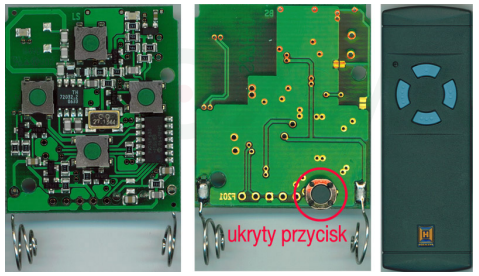


Fig. 5

Hormann zaś, dodał ukryty przycisk w pilocie, którym można wylosować kod pilota (w tym przypadku wirtualny DIPswitch posiadał aż 42 pozycje). Ukrytym przyciskiem można również przywrócić kod fabryczny pilota.



No, ale przecież nie widać kodu ustawionego w sposób elektroniczny! Gdy nie widać wirtualnego DIPswitcha, trudno ustawić taki sam kod w odbiorniku i trudno dorobić pilota.

Oczywiście wiecie co zrobiono, w odbiorniku dodano małą, tym razem elektroniczną pamięć jednego kodu pilota i przycisk (zazwyczaj czerwony), który wprowadzał odbiornik w specjalny stan zwany stanem rejestracji / nauki i w czasie której, należało zazwyczaj po prostu nacisnąć przycisk pilota.

No ale jak dorobić pilota - przecież pilot jest nadajnikiem i nie posiadał już DIPswitcha!

Wbudowano więc do pilota bardzo prosty, bardzo mało czuły odbiornik, który potrafił jednak odebrać sygnał innego pilota z kilku centymetrów, co zupełnie wystarczyło do wymiany informacji miedzy pilotami tzw. uczenie pilota od pilota.

Tak dorabia się prawie wszystkie piloty Hormanna, Ditec GOL4C, CAME TOP i TAM i wiele wiele innych.

Dla Państwa informacji:

Nice FLO	10 pozycji DIPswitch fizyczny
DITEC GOL 4C	10 pozycji DIPswitch wirtualny lub fizyczny
CAME TOP	10 pozycji DIPswitch wirtualny
CAME TAM	22 pozycji DIPswitch wirtualny
Hormann	42 pozycji DIPswitch wirtualny

Największą wadą sytemu stałokodowego jest duża łatwość przechwycenia transmisji pilota oryginalnego i wyemitowanie go, bądźmy poprawni politycznie, przez osobę nieuprawnioną.

Łatwo też poza Hormannem złamać wyżej wymienione systemy tzw. brutalnym atakiem (ang. brute force - wysłanie wszystkich możliwych kodów tzw. całej przestrzeni kodowej).

Zaletą systemu stałokodowego jest jego niezawodność, prostota, oraz łatwość integracji z innymi systemami np. popularnym w USA i spotykanym w Europie systemem HOMELINK (pilot zintegrowany z autem).

No ale w połowie lat osiemdziesiątych w Republice Południowej Afryki w firmie Nanoteq pracował pewien Pan - dr. Frederick Bruwer.

Jego pomysł, w niezmienionej od ponad trzech dekad formie, wykorzystuje świat i nic nie wskazuje na to żeby to się miało wkrótce zmienić. Jego dojrzały pomysł nazywa się KODEM ZMIENNYM Keeloq.

Kod zmienny

Zadaniem pilota zdalnego sterowania jest przekazanie rozkazu do sterownika.

Pilot do telewizora przesyła tylko kod rozkazu (kod naciśniętego klawisza) i dlatego steruje wszystkimi podobnymi telewizorami pozostającymi w zasięgu jego działania.

My chcemy, aby podobne sterowniki w pobliżu nie reagowały na naszą transmisję.

Jak zrobić żeby otwierała się tylko nasza brama?

W naszej transmisji powinien być zawarty nie tylko rozkaz (kod naciśniętego klawisza), ale również numer urządzenia które ma nasz rozkaz wykonać.

Piloty z kodem stałym pięknie i dokładnie spełniają te warunki.

Po co więc kod zmienny?

Kod zmienny ma tylko jeden cel – istotnie zwiększyć bezpieczeństwo.

Naciśnięcie pilota radiowego powoduje wysłanie sygnału radiowego, który może odebrać nie tylko odbiornik w sterowniku, ale również każdy odbiornik znajdujący się w zasięgu.

Jeżeli zarejestrujemy transmisję która np. otworzyła bramę, to jeżeli wyślemy ją ponownie to brama oczywiście się otworzy.

Na rynku istnieją piloty zwane klonerami – samokopiującymi – duplikatorami, które służą do dorabiania pilotów z kodem stałym. Czułość odbiornika radiowego który zawierają, jest niewielka – odbierają sygnał z tylko kilku centymetrów. Jeżeli zastąpimy ich kiepski odbiornik, odbiornikiem standardowym (czułym), to możemy odebrać sygnał z oryginalnego pilota ze znacznej odległości i zdalnie dorobić pilota. No cóż, właściciel oryginalnego pilota może przecież nie zdawać sobie z tego sprawy....

Co zrobić żeby podsłuchany sygnał radiowy, który otworzył bramę stał się dla podsłuchującego bezużyteczny?

Rozwiązaniem jest np. dodanie do informacji zawartej w transmisji pilota, obok niezbędnej informacji (tj. informacji o naciśniętym klawiszu i numerze odbiornika), również aktualnej DATY (rok, miesiąc,...sekunda). Sterownik, po odebraniu transmisji radiowej, sprawdza czy DATA zawarta w transmisji jest aktualna i jeśli TAK wykonuje rozkaz, a jeśli nie to nie.

Jest to (moim zdaniem) najbardziej oczywisty KOD ZMIENNY.

Spełnia wymagane warunki – wysłanie podsłuchanej transmisji nie zadziała – DATA w transmisji będzie starsza – nieaktualna.

Techniczną niedogodnością tego rozwiązania jest potrzeba synchronizacji zegara pilota i zegara sterownika.

W praktyce nie używa się DATY.

W praktyce do każdej transmisji zamiast DATY, dodaje się liczbę, która po każdym naciśnięciu przycisku pilota jest zwiększana o 1 – tą liczbę nazywa się numerem emisji.

Sterownik po wykonaniu rozkazu, zapamiętuje numer emisji rozkazu i jeżeli odbierze transmisję z tym samym lub mniejszym numerem emisji – nie reaguje, jeżeli nr emisji jest nieco większy wykonuje rozkaz pilota. Nieco – wyjaśnię dalej.

Jesteśmy już bliżej stosowanego w praktyce KODu ZMIENNEGO.

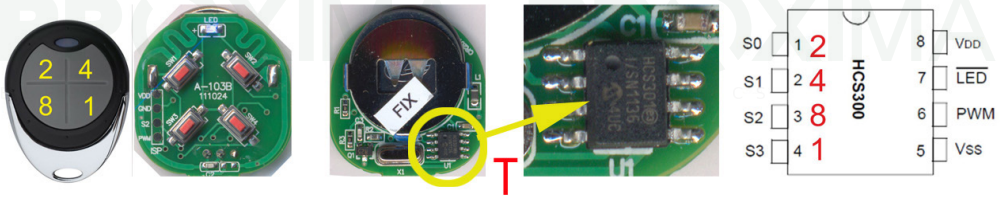
Co jest jeszcze słabe w tym pomyśle?

No cóż przesłanie numeru emisji w sposób jawny, niezakodowany, umożliwia sprytnemu podsłuchujący łatwą modyfikacje numeru emisji. Jeżeli dobrze zakodujemy numer emisji podsłuchujący będzie miał kłopot z właściwą modyfikacją podsłuchanej transmisji. Jeszcze lepiej gdy dobrze zakodujemy całą transmisję. Jak zwykle jednak diabeł siedzi w szczegółach.

Układ HCS

Układ HCS amerykańskiego potentata w dziedzinie mikroprocesorów firmy MICROCHIP jest niezwykle popularnym i zarazem chyba jedynym na świecie układzie scalonym, służącym do bezprzewodowego zmiennokodowego zdalnego sterowania (nie licząc kilku odmian tej wersji). W znakomitej większości wykorzystywanym w motoryzacji (AUDI, PORSCHE, TOYOTA...).

Po rozkręceniu pilota można odszukać ośmionóżkowy układ scalony z opisem HCS 200, HCS300, HCS 301 itp. - **T** to nasz dzisiejszy bohater.

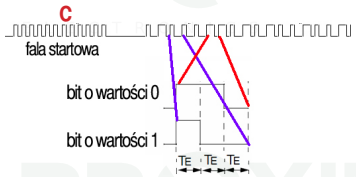


Jeżeli dołączymy rejestrator cyfrowy do odbiornika radiowego i naciśniemy np. klawisz nr4 pilota zobaczymy charakterystyczny szczerbaty przebieg:

Każda transmisja zaczyna się falą startową **C**.

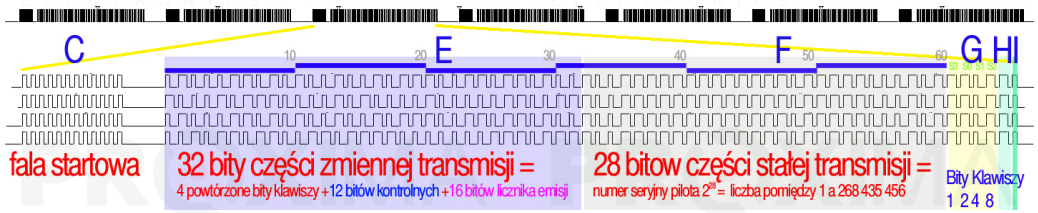
Dzięki zawsze takie samej fali startowej, zwaną oryginalnie preambułą (rozbiegówką):
- odbiornik ma czas na dostosowanie swojego wzmocnienia do poziomu odebranego sygnału (ARW - automatyczna regulacja wzmocnienia ma swoją stałą czasową),
- procesor odbiornika zaś, ma ułatwioną detekcję początku transmisji.

Po fali startowej HCS nadaje zwartą grupę 66 bitów informacyjnych identycznych w każdej kolejnej grupie, tak długo jak trzymamy przycisk.



Bit matematyczny (cyfra 0 lub 1), zamieniany jest przez układ HCS na szerszy (dłużej trwający), lub węższy (krócej trwający) sygnał radiowy.

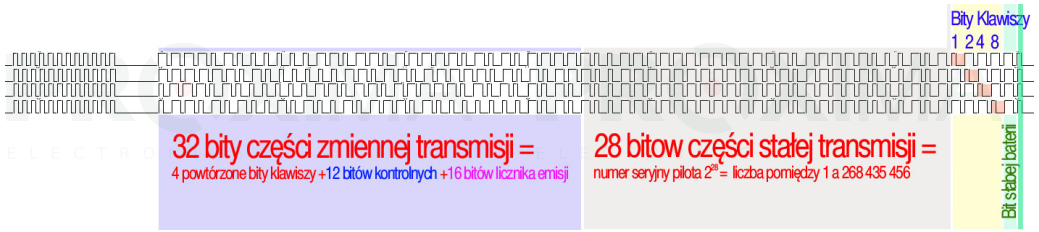
Obrazek poniżej pokazuje 4 kolejne emisje, po naciśnięciu klawisza numer 4 pilota. Wyraźnie widać że pierwsze 32 bity się zmieniają, a bity pozostałe są takie same.



Pierwsze 32 bity zmieniają się zawsze po każdym naciśnięciu przycisku - E. Zawierają one zakodowane 4 bity przyciśniętych klawiszy - 12 bitów kontrolnych i 16 bitów licznika emisji (zwiększanego o +1 po każdym naciśnięciu przycisku pilota). Licznik emisji po osiągnięciu 65536 – zaczyna od początku.

Kolejne 28 bitów są zawsze stałe dla pilota i tworzą numer seryjny pilota od nr 1 do nr 268 435 456, nadawany podczas programowania układu HCS przez wytwórcę pilota - F.

Obrazek poniżej pokazuje jak zmieniają się bity klawiszy, w zależności od tego który klawisz piloyta został naciśnięty.



Można naciskać jeden, dwa lub trzy dowolne przyciski równocześnie, tworząc 14 kombinacji. Oznacza to że, układ HCS 300 może być maksymalnie pilotem 14 kanałowym.

Naciśnięcie czterech klawiszy jednocześnie, zmienia działanie układu HCS i zamiast 32 bitowej części zmiennej przesyła zawsze te same 32 bity (zapisane podczas programowania przez wytwórcę pilota do jego pamięci). Te 32 bity nazywane są przez producenta SEED (ziarno).

Bit 65 jest bitem stanu baterii (1- bateria słaba, 0 bateria dobra).

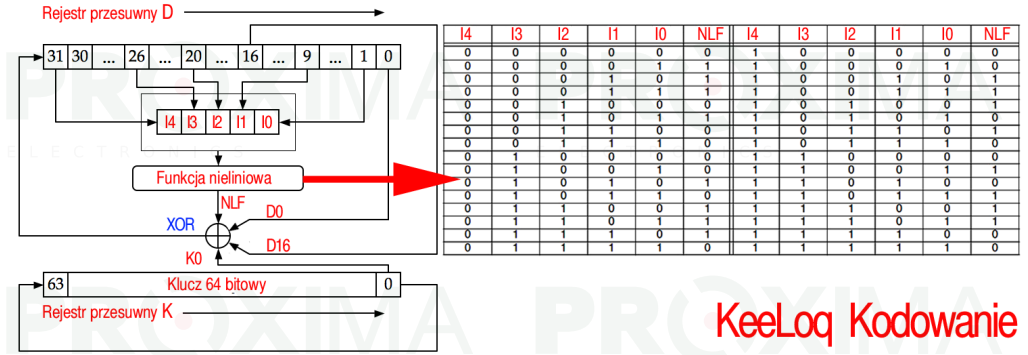
Bit 66 miał historycznie rożne znaczenia, ale teraz najczęściej służy do tego żeby procesor wiedział gdzie kończy się bit 65.

Kodowanie Keeloq

Podczas programowania, producent pilotów wprowadza kilka liczb do układu HCS. Najważniejsze z nich to wspomniany już 28 bitowy numer seryjny i 64 bitowy klucz szyfrującym (ang. encryption key), 12 bitów kontrolnych i 32 bity SEED.

Po każdym naciśnięciu przycisku układ HCS zaczyna skomplikowany proces obliczeniowy mający na celu wyliczenie 32 bitów części zmiennej na podstawie 32bitów (klawisze + bity kontrolne + numer emisji) i 64 bitów klucza szyfrującego.

Najpierw ładuje do 32 bitowego rejestru przesuwnego **D** jawne 32 bity na które składają się wspomniane 4 bity klawiszy+12 bity kontrolne i najważniejsze 16 bitów numeru emisji. Następnie do rejestru przesuwnego **K** ładuje 64 bity klucza szyfrującego.



KeeLoq Kodowanie

I zaczynają się obliczenia...

1. Procesor z rejestru **D** pobiera 5 bitów z pozycji 1 - 9 - 20 - 26 i 31 i za pomocą funkcji nieliniowej zamienia 5 **I0-I4** bitów na jeden bit **NLF**.

2. Z rejestru klucza szyfrującego **K** z pozycji 0 pobierany jest bit **K0** .

3. Z czterech bitów **NLF, D0**, **D16** i **K0** wyznacza bit **XOR** (procesor liczy ilość bitów o wartości 1, jeżeli jedynek brak, są dwie, lub cztery **XOR** = 0, jeżeli jest jedna lub trzy jedynki, **XOR** =1 jest to funkcja XOR)

4. Przesuwa o jedną pozycję w prawo bity w rejestrze **D**, tracąc dawny bit z pozycji 0 i tworząc wolne miejsce na pozycji 31, na które wpisuje bit **XOR**.

5. Przesuwa w prawo o jedną pozycję bity klucza szyfrującego **N** wpisując dawny bit z pozycji 0 na pozycje 63.

7. Wykonuje 528 razy działania z punktów 1- 5.

Po wykonaniu wszystkich opisanych wyżej działań, to co znajduje się teraz w rejestrze przesuwnym **D**, jest 32 bitami przesyłanymi na miejscu części zmiennokodowej - przyznacie niezwykle mocno zakodowane 32 bity (klawisze + bity kontrolne + numer emisji).

Dekodowanie Keeloq

Odbiornik po odbiorze transmisji pilota, dekoduje, identycznym 64 bitowym kluczem szyfrującym, część zmienną i uzyskuje 32 bity na które składają się:

- 4 bity klawiszy
- 12 bitów kontrolne
- 16 bitów numeru emisji.

I teraz odbiornik;

1. Sprawdza czy bity klawiszy w części zakodowanej i bity przesłane jawnie są identyczne - a powinny oczywiście być identyczne.

2. Sprawdza czy wpisane przez producenta pilota do układu HCS 12 bitów kontrolnych są takie jak być powinny. Najczęściej jest to część numeru seryjnego.

Jeżeli sprawdzanie w punktach 1 i 2 dały wynik pozytywny, odbiornik uznaje, że transmisja został prawidłowo odebrana i rozkodowana. Jeżeli wystąpił błąd transmisja zostaje zignorowana.

Pora na zinterpretowanie numeru emisji.

Jeżeli rozkaz który przyszedł, ma numer nieco większy (zazwyczaj max od 8 do 64) niż poprzedni, który odbiornik odebrał, zaakceptował i zapamiętał to odbiornik wykonuje rozkaz wynikając z bitów klawiszy i zapisuje nowy zaakceptowany numer emisji.

Jeżeli numer emisji który został odebrany jest mniejszy lub równy od numeru zaakceptowanego wcześniej przez odbiornik, to ignoruje rozkaz jako już wykorzystany. **Jest najważniejsza decyzja idei zmiennego kodu.**

Jeżeli numer emisji który został odebrany jest dużo większy niż poprzedni, odbiornik zapisuje go na boku (nie jako numer zaakceptowany), ale rozkazu nie wykonuje.

Jeżeli kolejna emisja będzie o np. jeden dwa lub trzy (ale nie więcej) większa od zapisanej na boku, to odbiornik wykona rozkaz i zmieni na nowy zaakceptowany numer emisji.

Skąd ta ostrożność co do niewielkiego wzrostu kolejnego numeru emisji, po co bity kontrolne, po co porównywanie bitów klawiszy z części jawnej z bitami klawiszy w części zakodowanej?

Spróbujmy na to odpowiedzieć – jeżeli jeszcze to czytacie.

Załóżmy że 32 bity zakodowane zawierają tylko 32 bitowy licznik emisji, a odbiornik reaguje na dowolnie większy numer emisji od zaakceptowanego poprzednio; idea zmiennego kodu.

Jesteśmy bezpieczni przecież kodowanie jest nie złamania!

Niestety nie, choć kodowanie jest bezpieczne, dlaczego?

Ano dlatego, że złodziej odbiera dowolną transmisję oryginalnego pilota i łatwo ustala numer seryjny (jest przecież niekodowany).

Wysyła transmisję z właściwym numerem seryjnym i z losową, dowolną częścią zmienną.

Odbiornik dekoduje super zakodowaną informację i zawsze wychodzi jakaś liczba 32 bitowa i jest ona, albo większa od zaakceptowanego poprzednio numeru emisji (odbiornik wykonuje rozkaz), albo jest mniejsza lub równa (odbiornik ignoruje rozkaz).

Niesamowite, pomimo potężnego kodowania, statystycznie co druga przypadkowa część zmienna jest zaakceptowana i otwiera bramę.

Klucze szyfrujące.

Procedura Keeloq wymaga klucza szyfrującego o długości 64 dowolnych bitów.

Producent wymyśla sobie najtajniejszy z tajnych swój własny ciąg 64 bitów będący kluczem producenta tzw. manufacturer key.

Stały klucz szyfrujący.

Najprostszy pomysłem (wykorzystywanym przez dużych i małych producentów pilotów - przez grzeczność ich nie wymienimy) jest wpisanie do układu HCS klucza producenta.

Wadą tego rozwiązania jest fakt że w każdej transmisji (jako część zmienna) przesyłamy ten klucz nieźle pomieszany z 32 bitami (bity klawiszy + bity kontrolne + numer emisji).

Jeżeli inteligentny przeciwnik wyodrębni klucz szyfrujący (np. kupi pilota i poda go intensywnej analizie) to uzyska w ten sposób dostęp do wszystkich urządzeń sterowanych pilotami tego producenta, które wyprodukował on w swojej historii.

Klucz szyfrujący zależny od numeru seryjnego.

Najszerzej rozpowszechnionym sposobem jest wpisanie do układu HCS nie klucza producenta, a klucza który powstał przez mieszanie kodowaniem Keeloq (choć niekoniecznie w ten sposób) klucza producenta i seryjnego numeru pilota.

Przesyłamy więc, nie oryginalny klucz producenta, ale jego mieszaninę z numerem seryjnym pilota - każdy klucz szyfrujący jest więc inny.

Inteligentny przeciwnik musi wyodrębnić klucz szyfrujący tylko na podstawie przechwyconych oryginalnych transmisji, ale nawet wówczas, uzyska w ten sposób dostęp tylko do urządzeń tego producenta sterowanych tym i tylko tym pilotem.

Klucz szyfrujący z SEEDa.

Jak wspomnieliśmy wyżej, naciśnięcie czterech klawiszy jednocześnie, zmienia działanie układu HCS i zamiast 32 bitowej części zmiennej przesyła zawsze te same 32 bity (zapisane podczas programowania przez wytwórcę pilota do jego pamięci). Te 32 bity nazywane są przez producenta SEED (ziarno). W procesie rejestracji pilota do odbiornika przesyła się SEEDA, a odbiornik na podstawie klucza producenta i SEEDa wylicza klucz szyfrujący.

Podczas normalnej pracy, pilot nie przesyła się w żadnej postaci klucza producenta.
Jest to najbezpieczniejszy klucz szyfrujący oferowany przez system KeeLoq
Z tego trybu korzysta między innymi BFT - naciśniecie ukrytego przycisku w pilocie BFT, jest naciśnięciem czterech przycisków jednocześnie – można to sprawdzić, ale potrzebny jest pilot BFT z czteroma klawiszami.

Sposoby weryfikujące kod zmienny.

1. Jeżeli radio ma możliwość wyłączenia trybu rejestracji stałokodowej – należy ją wyłączyć.

Jeżeli radio rejestruje wówczas tylko piloty z HCSem systemowe, a nie rejestruje pozostałych pilotów z HCSem to my pewność, że radio zna klucz szyfrujący i potrafi odczytać część zmienno kodową i prawie na pewno pracuje zmiennokodowo.

2. Drugi, dosyć łatwy dla niektórych systemów sposób, to zarejestrować pilota w radioodbiorniku. Odłączyć zasilanie odbiornika i **wiele razy** nacisnąć zarejestrowany przycisk pilota. Wyłączone radio nie odbiera pilota.

Wiele dla DTMu oznacza minium 17 razy,

- dla FAAC FIX i FAAC RC minium 15razy,

- dla PROXIMy 32 razy,

- dla Nice Smilo aż 256 razy,

a dla CAME SPACE naciskałem ponad 600 razy i eksperyment się nie udał, mają za szerokie okno, ale kod jest kodem zmiennym.

Producent MICROCHIP zaleca **17 razy**.

Następnie dołączamy zasilanie odbiornika, czekamy aż odbiornik osiągnie stan gotowości (przejdzie do normalnej pracy) i naciskamy zarejestrowany przycisk pilota, jeżeli odbiornik nie zareagował na pierwsze naciśnięcie, a zareagował dopiero na powtórne naciśnięcie – to mamy pewność że odbiornik pracuje w systemie zmiennokodowym....

Pozdrawiam

M

www.proxima.pl

PROXIMA
ELECTRONICS