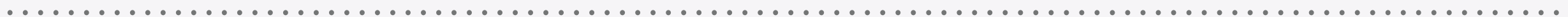


KEYLESS CAR



WEJŚCIE DO POJAZDU

- Zamki mechaniczne

WEJŚCIE DO POJAZDU

- Zamki mechaniczne
- RKE system

WEJŚCIE DO POJAZDU

- Zamki mechaniczne
- RKE system
- smart keys (PKES)

URUCHOMIENIE AUTA

Uruchomienie auta:

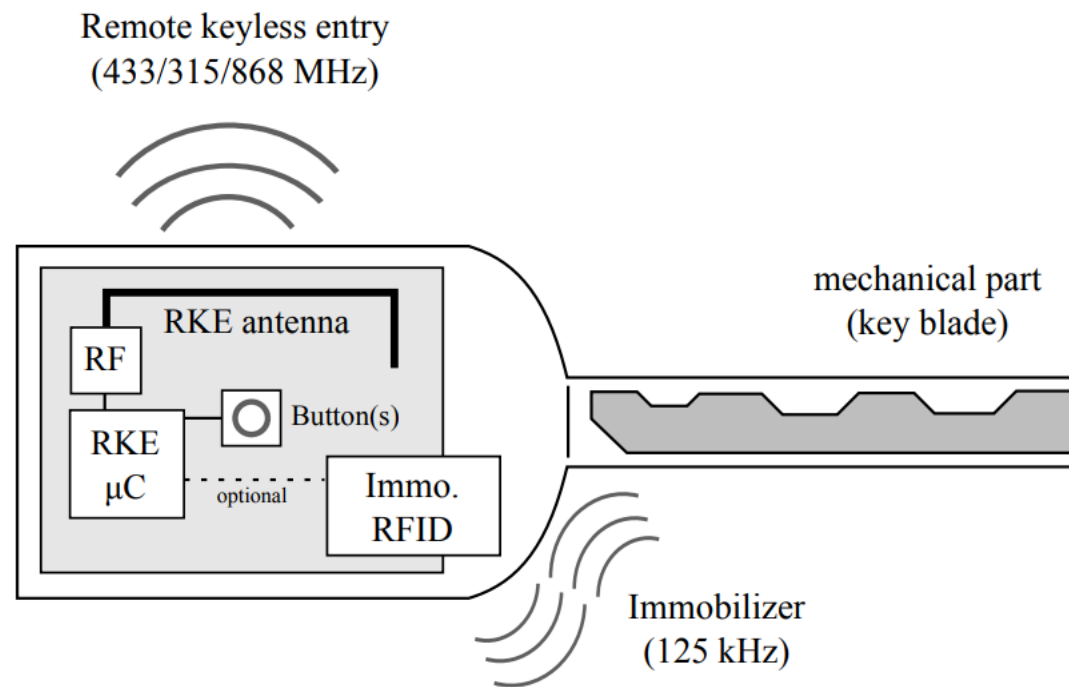
- Na początku trzeba do niego wejść

URUCHOMIENIE AUTA

Uruchomienie auta:

- Na początku trzeba do niego wejść
- W większości aut znajduje się mechaniczny zamek

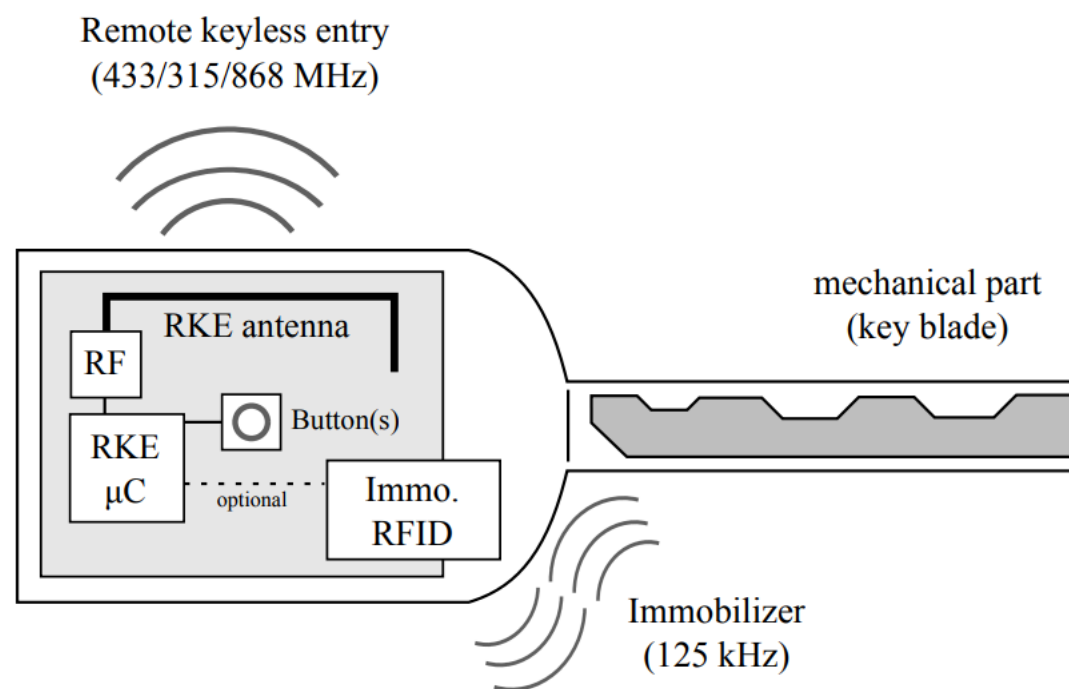
URUCHOMIENIE AUTA



Uruchomienie auta:

- Na początku trzeba do niego wejść
- W większości aut znajduje się mechaniczny zamek
- W nowszych autach mamy immobilizer

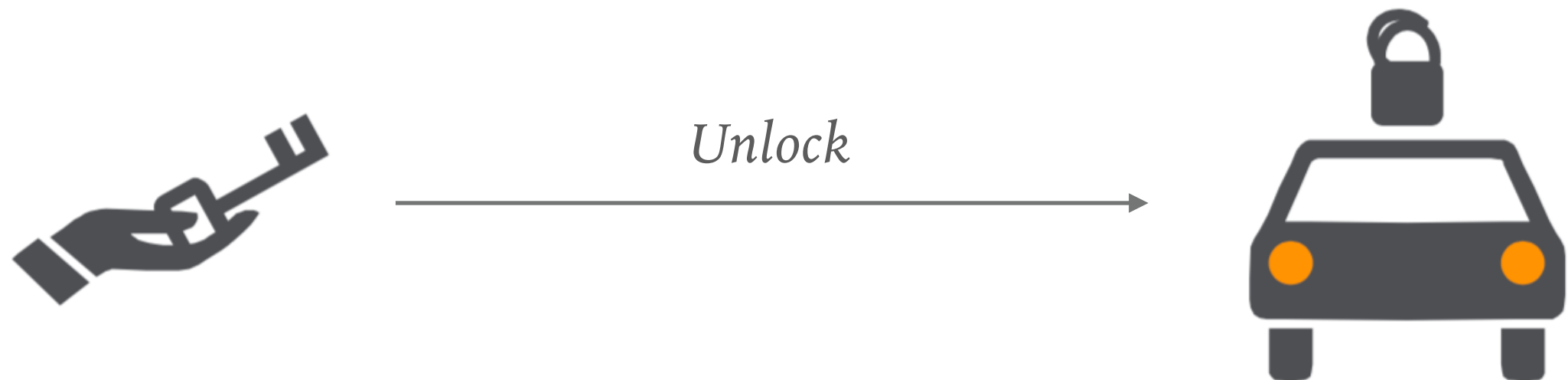
URUCHOMIENIE AUTA



Uruchomienie auta:

- Na początku trzeba do niego wejść
- W większości aut znajduje się mechaniczny zamek
- W nowszych autach mamy immobilizer
- Bardziej luksusowe auta posiadają przycisk start/stop

RKE – REMOTE KEYLESS ENTRY



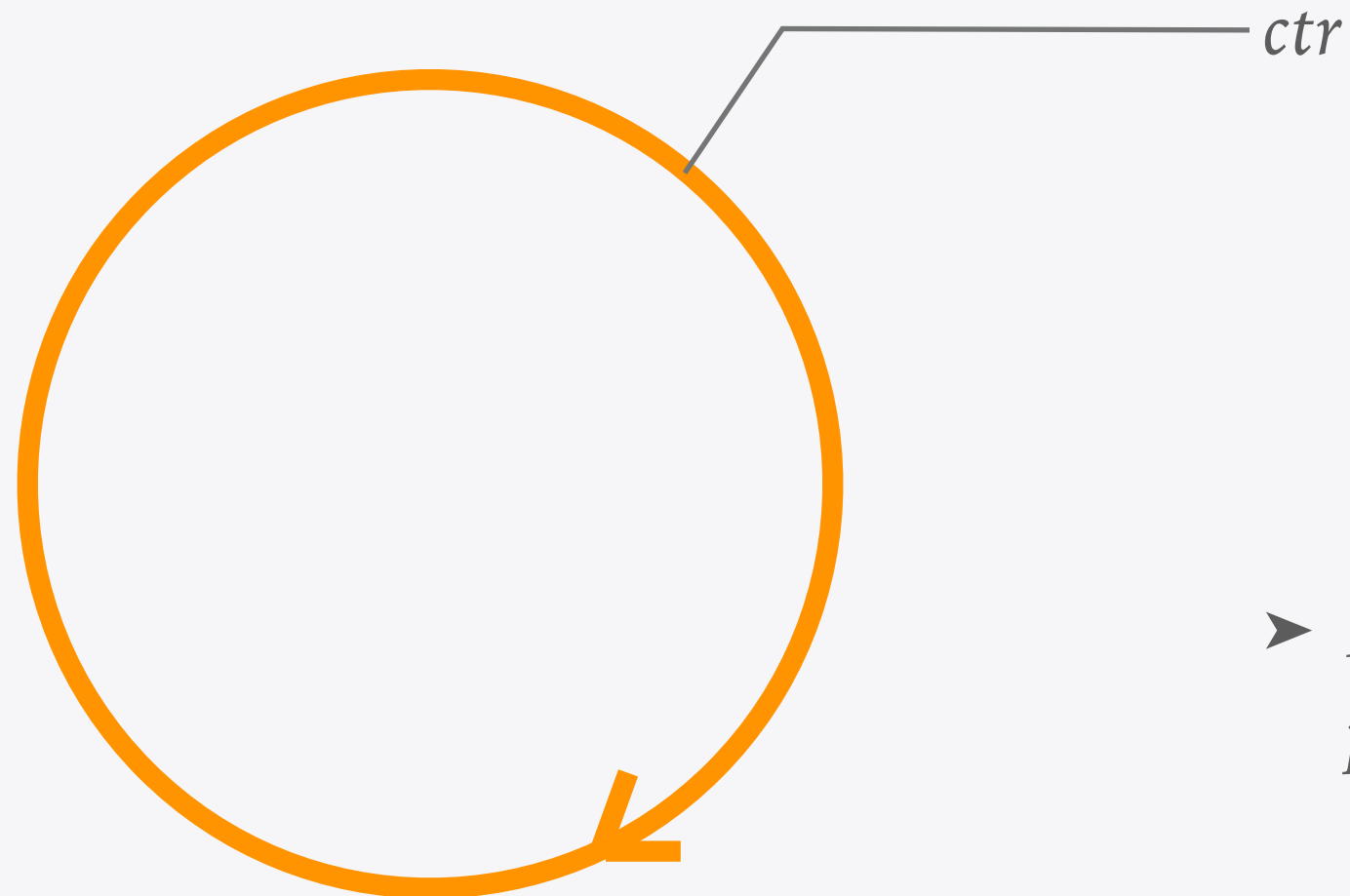
ROLLING CODE – GENERAL STUCTURE



Payload:

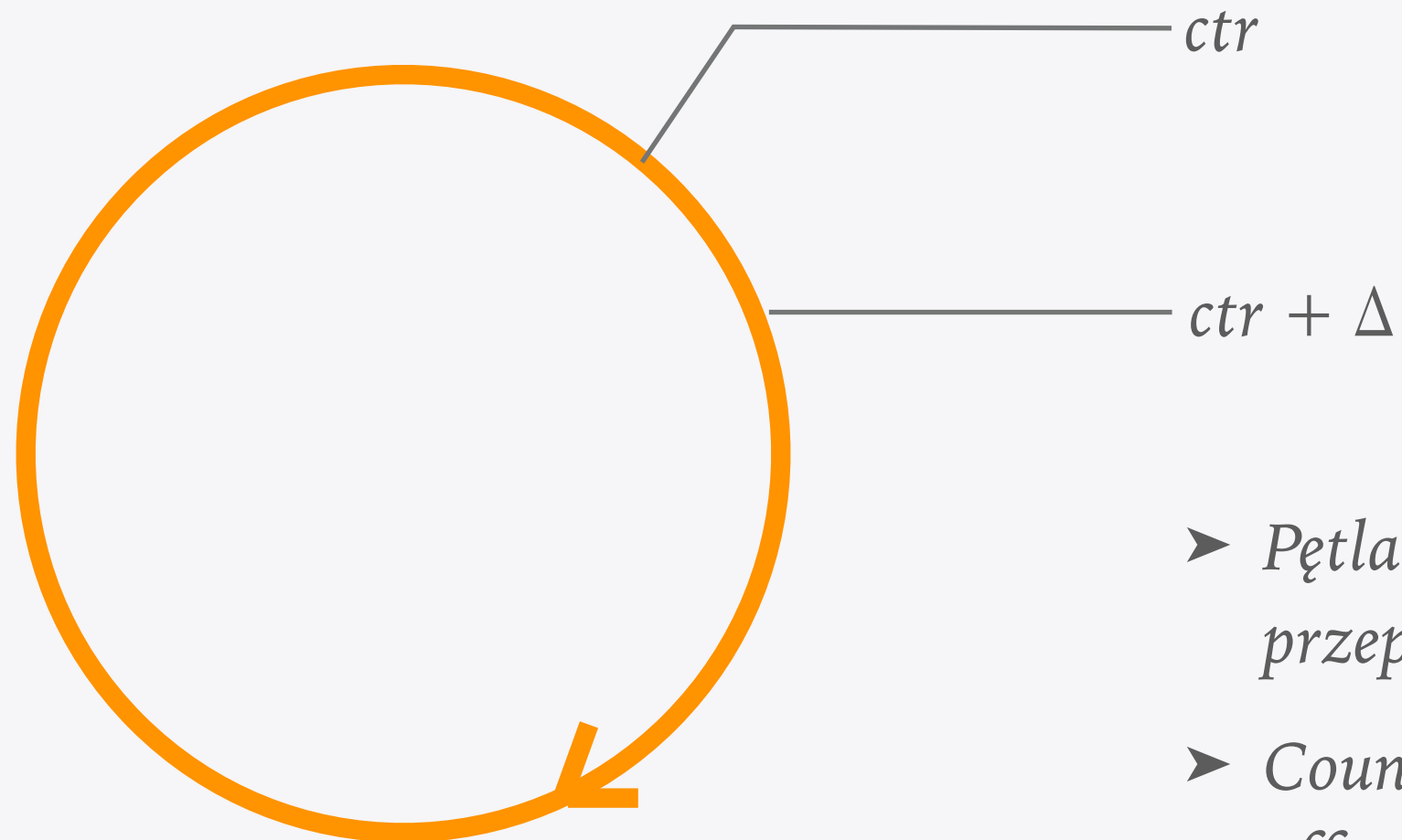
- *UID - Unique Identifier of the remote control*
- *Rolling counter value*
- *Pressed button (unlock/lock/open trunk)*

ROLLING CODE



- *Pętla zapobiega
przepelnieniu się licznika*

ROLLING CODE



- *Pętla zapobiega przepelnieniu się licznika*
- *Counter posiada niewielki offset*

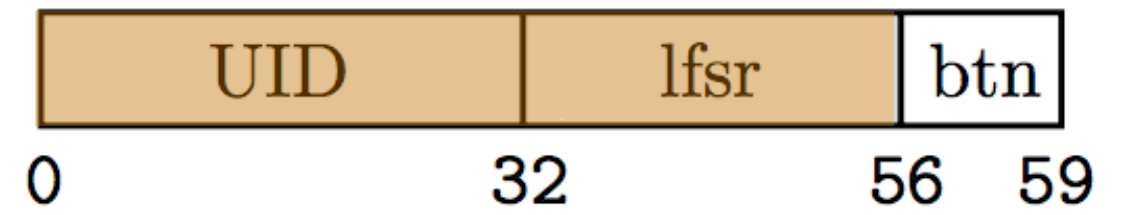
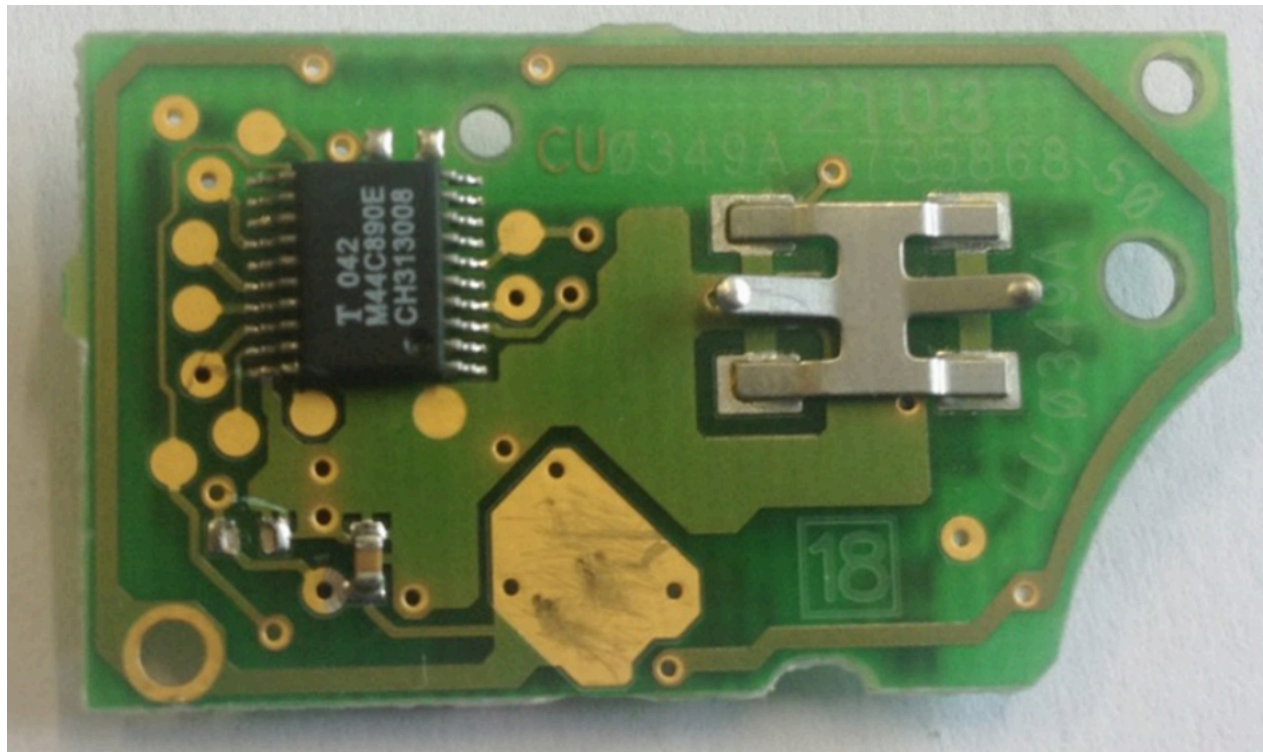
- Audi: A1, Q3, R8, S3, TT, other types of Audi cars (e.g. remote control 4D0 837 231)
- VW: Amarok, (New) Beetle, Bora, Caddy, Craver, e-Up, Eos, Fox, Golf 4, Golf 5, Golf 6, Golf Plus, JeHa, Lupo, Passat, Polo, T4, T5, Scirocco, Sharan, Tiguan, Touran, Up
- Seat: Alhambra, Altea, Arosa, Cordoba, Ibiza, Leon, MII, Toledo
- Škoda: City Go, Roomster, Fabia 1, Fabia 2, Octavia, Superb, YeG

VW GROUP

- Audi: A1, Q3, R8, S3, TT, other types of Audi cars (e.g. remote control 4D0 837 231)
- VW: Amarok, (New) Beetle, Bora, Caddy, Craver, e-Up, Eos, Fox, Golf 4, Golf 5, Golf 6, Golf Plus, JeHa, Lupo, Passat, Polo, T4, T5, Scirocco, Sharan, Tiguan, Touran, Up
- Seat: Alhambra, Altea, Arosa, Cordoba, Ibiza, Leon, MII, Toledo
- Škoda: City Go, Roomster, Fabia 1, Fabia 2, Octavia, Superb, YeG

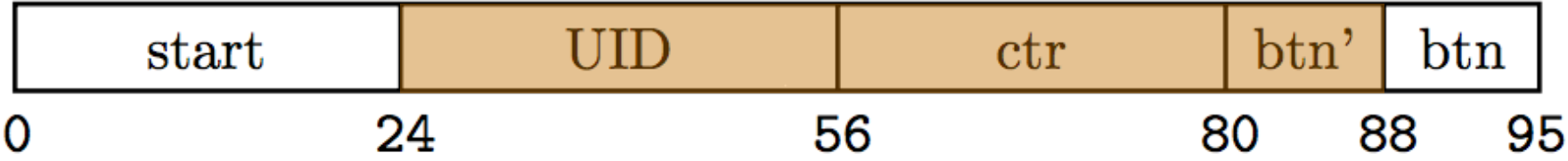
VW1

.....

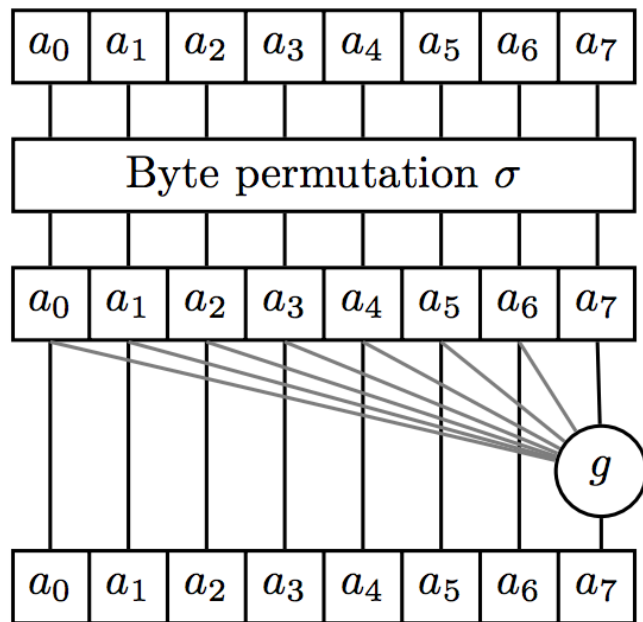
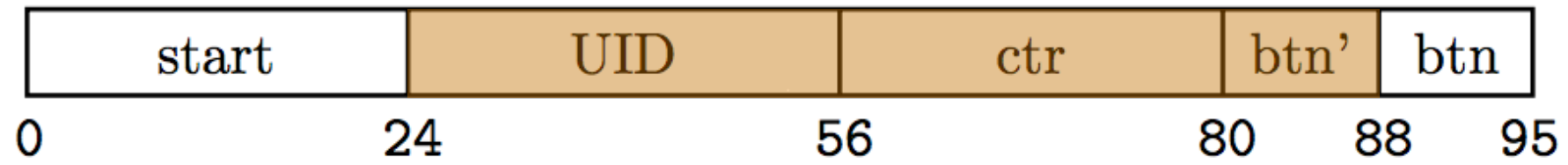


VW 2-3

.....

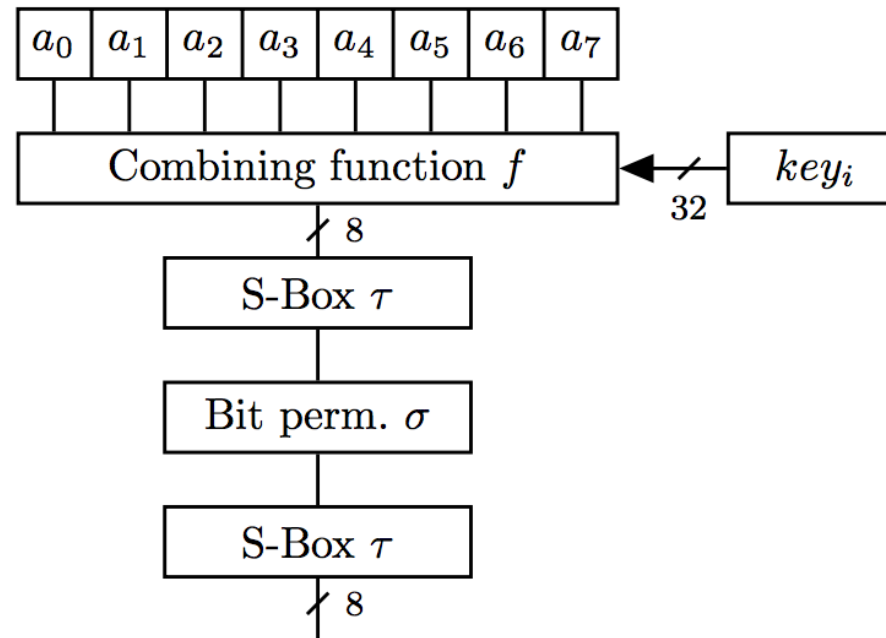
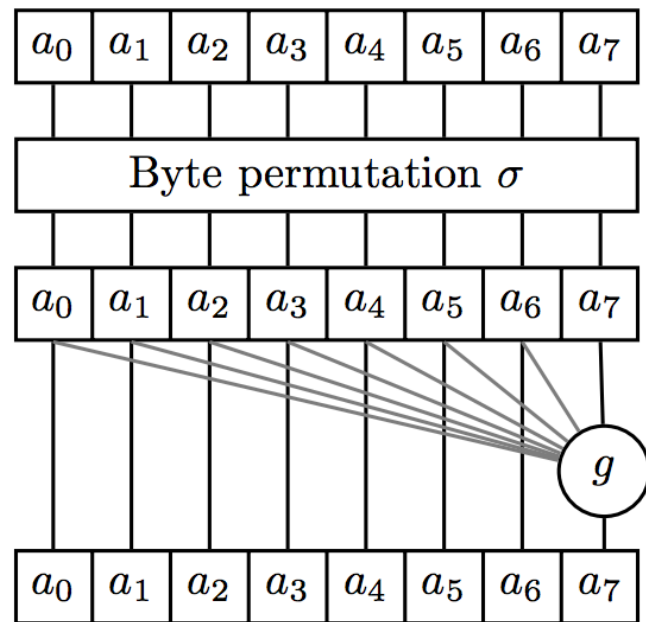
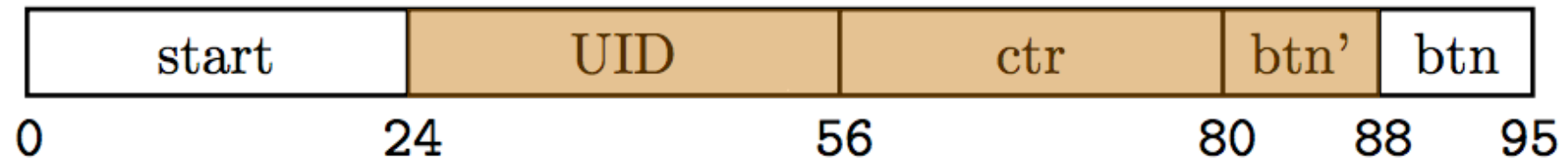


VW 2-3

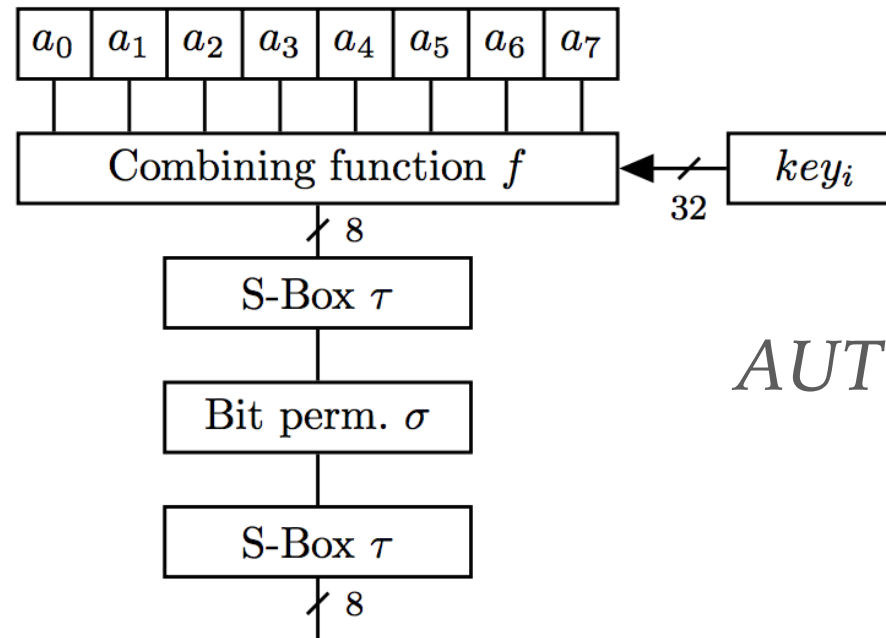
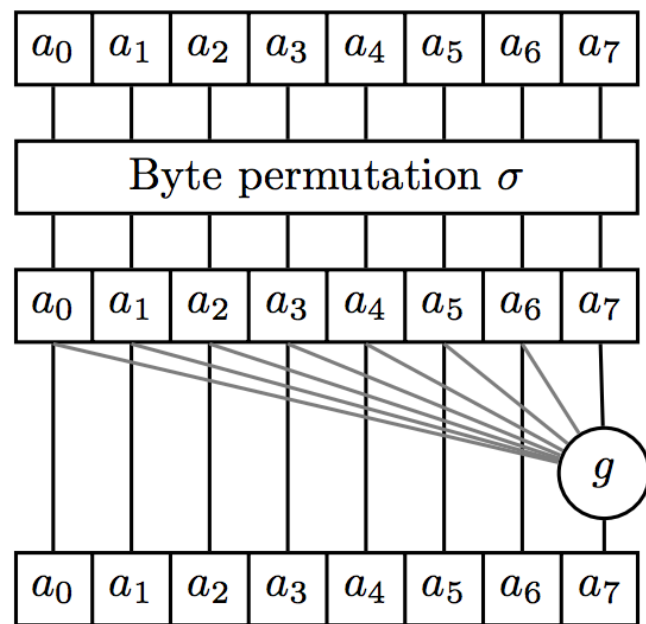
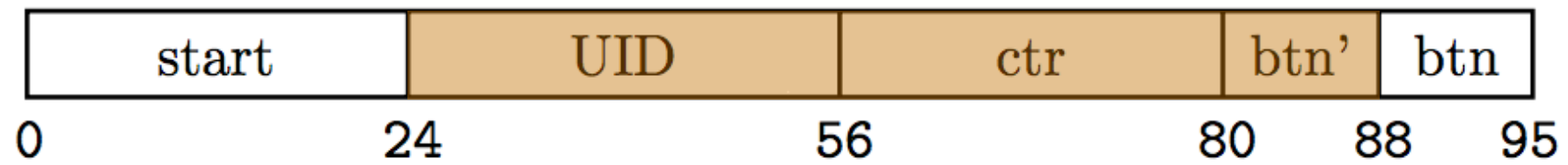


VW 2-3

.....

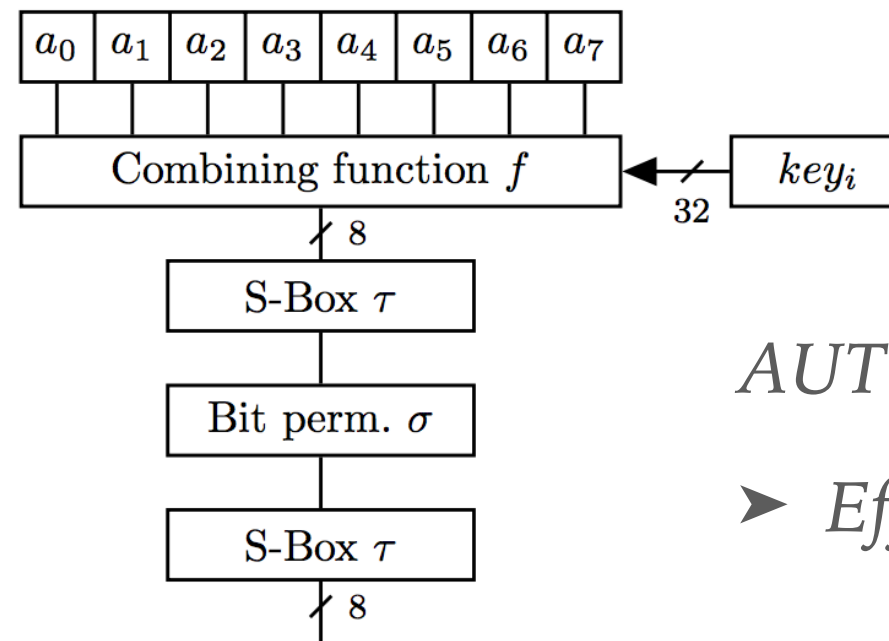
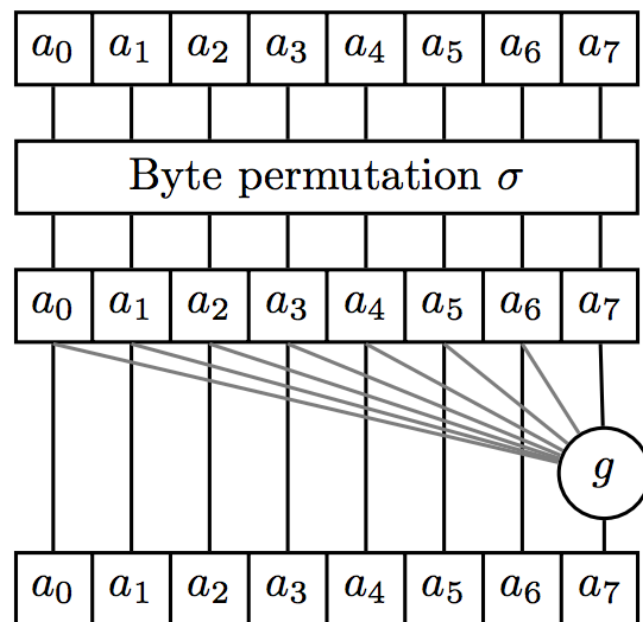
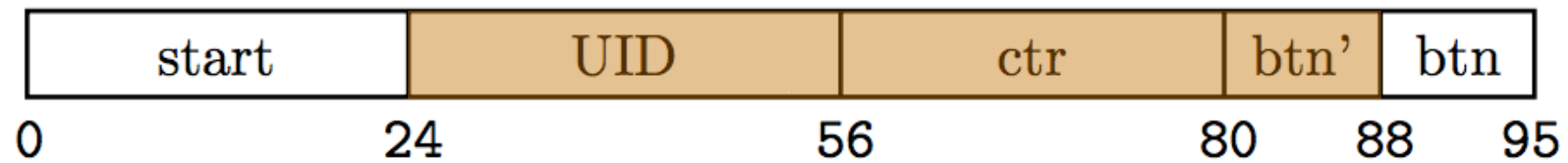


VW 2-3



AUT64 Block Cipher

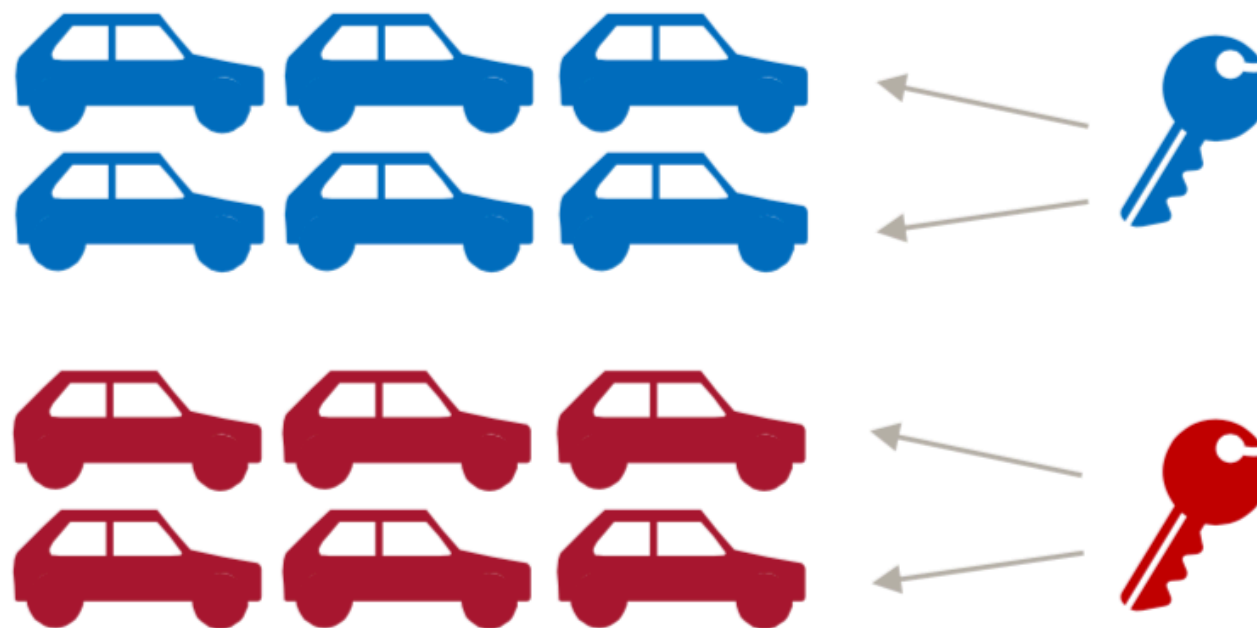
VW 2-3



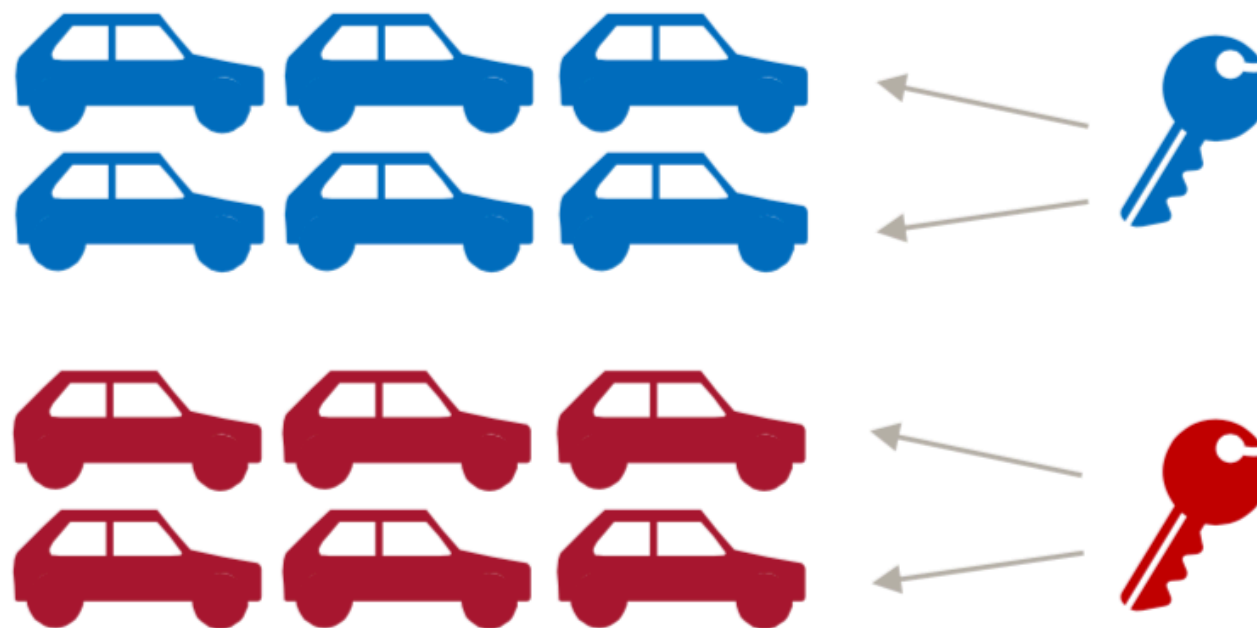
AUT64 Block Cipher

➤ *Effective key size = 91.55*

VW CIĄG DALSZY



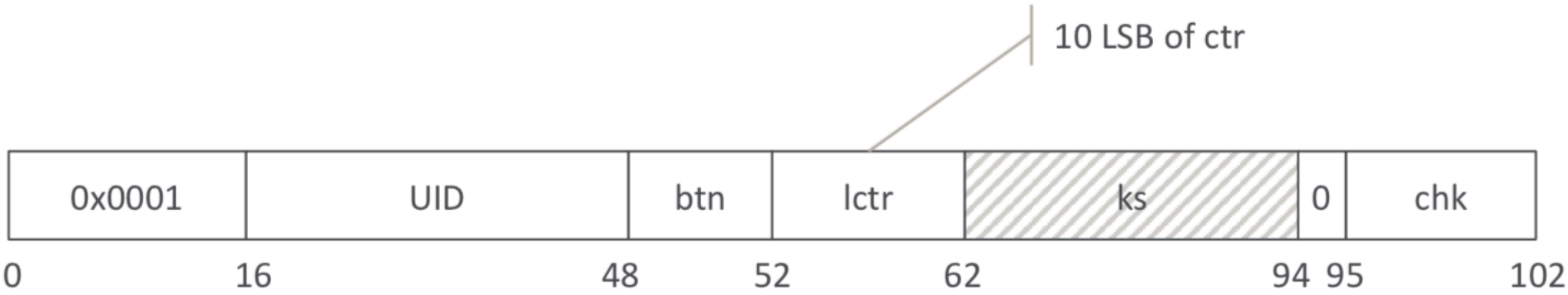
VW CIĄG DALSZY



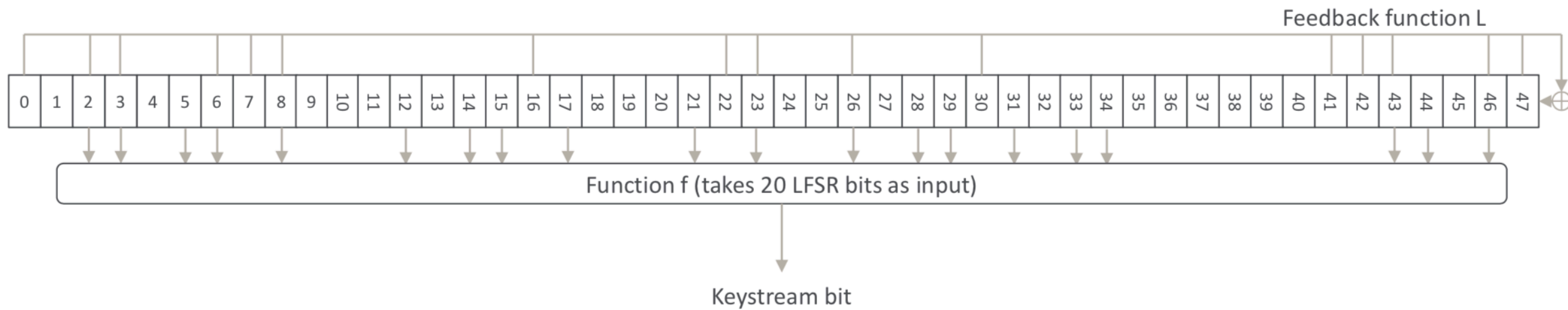
W VW 4 zamieniono szyfr na XTEA

HITAG2

.....

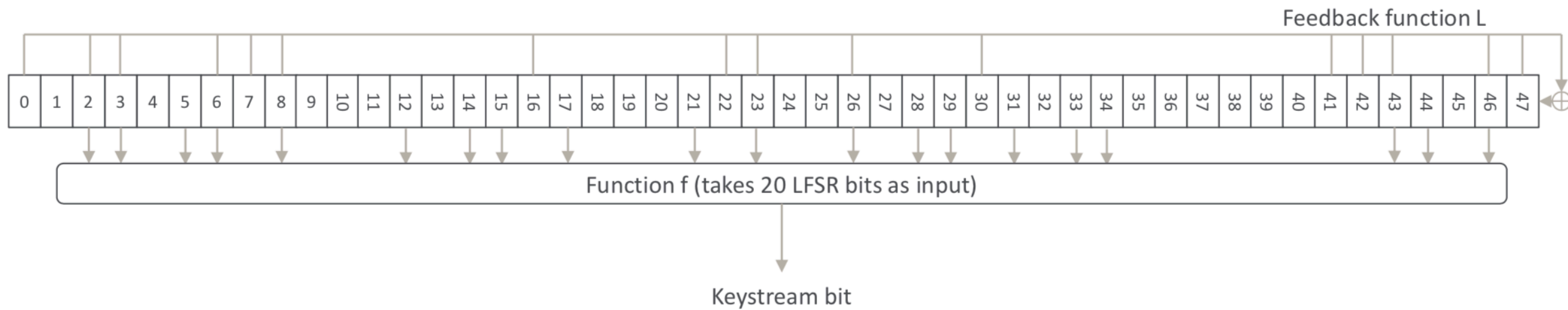


HITAG2



Do zainicjalizowania potrzebujemy:

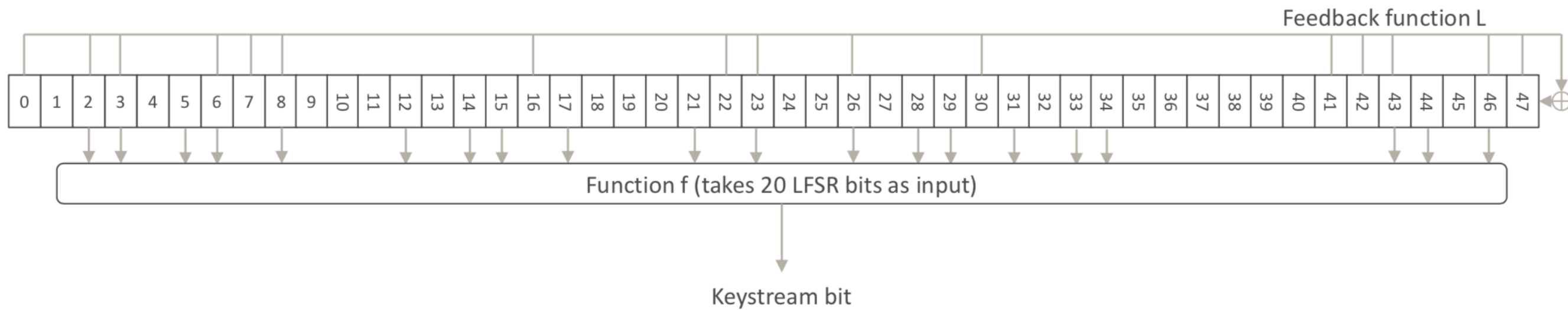
HITAG2



Do zainicjalizowania potrzebujemy:

➤ ID

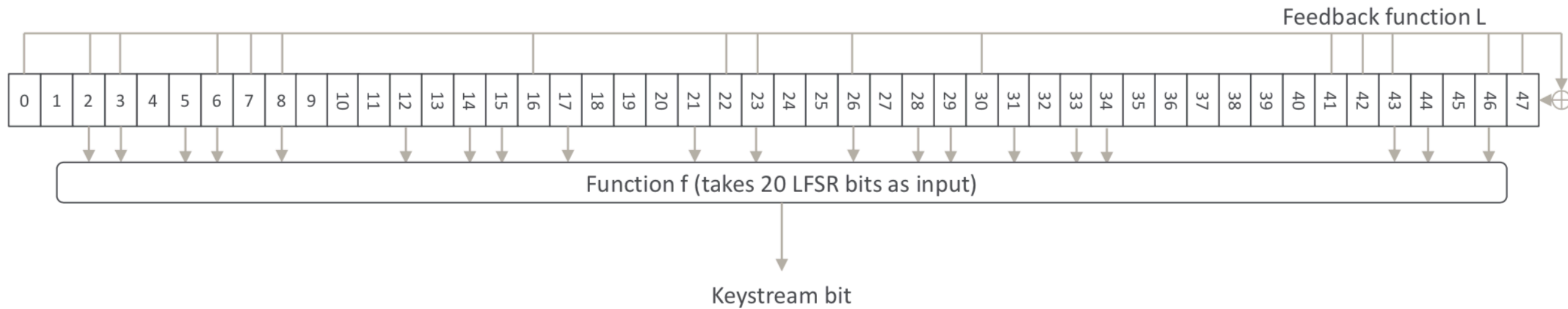
HITAG2



Do zainicjalizowania potrzebujemy:

- ID
- Klucz

HITAG2



Do zainicjalizowania potrzebujemy:

- ID
- Klucz
- $iv = ctr || btn$

UWAGI PRAKTYCZNE

Czas ataku - ok. 10 minut

UWAGI PRAKTYCZNE

Czas ataku - ok. 10 minut

Do wykonania potrzebujemy od 4 do 8 śladów. Aby je zdobyć możemy :

UWAGI PRAKTYCZNE

Czas ataku - ok. 10 minut

Do wykonania potrzebujemy od 4 do 8 śladów. Aby je zdobyć możemy :

- Zakłócić sygnał

UWAGI PRAKTYCZNE

Czas ataku - ok. 10 minut

Do wykonania potrzebujemy od 4 do 8 śladów. Aby je zdobyć możemy :

- Zakłócić sygnał
- Samochód zignoruje niepoprawny sygnał

UWAGI PRAKTYCZNE

Czas ataku - ok. 10 minut

Do wykonania potrzebujemy od 4 do 8 śladów. Aby je zdobyć możemy :

- Zakłócić sygnał
- Samochód zignoruje niepoprawny sygnał
- My przechwytujemy wysłany sygnał

UWAGI PRAKTYCZNE

Czas ataku - ok. 10 minut

Do wykonania potrzebujemy od 4 do 8 śladów. Aby je zdobyć możemy :

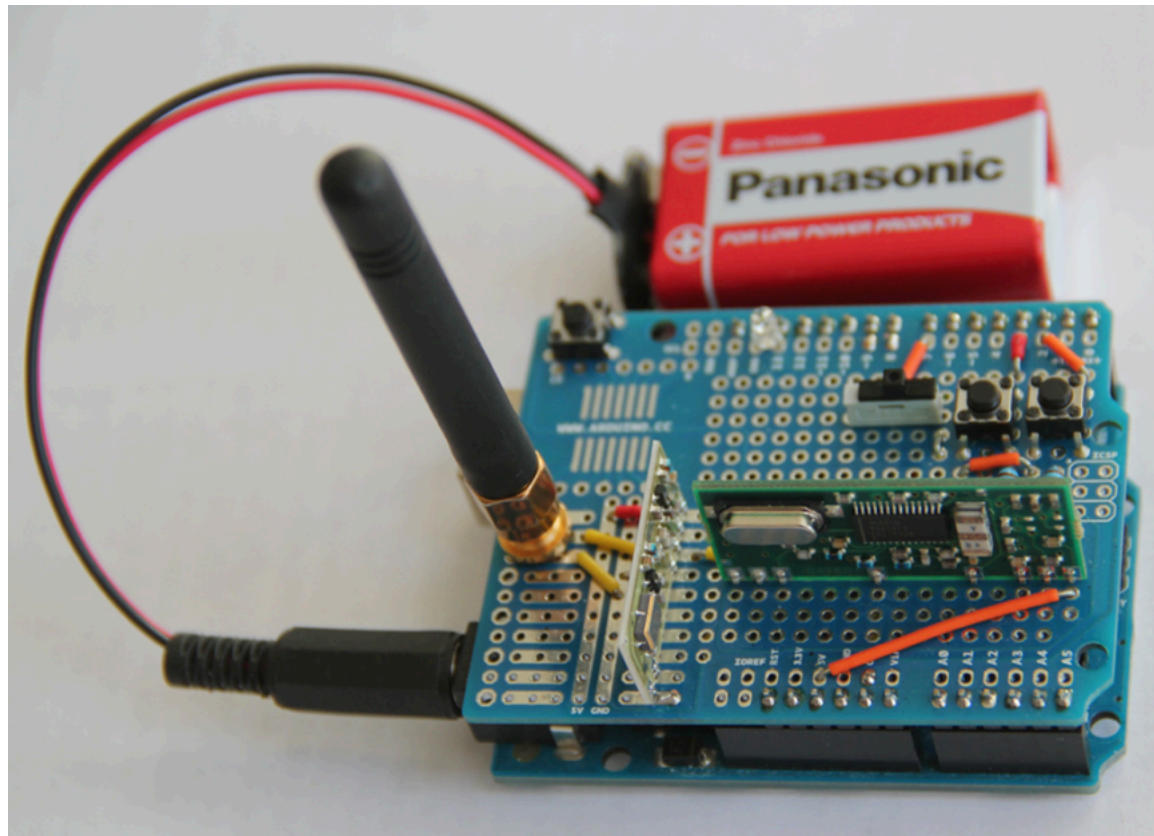
- Zakłócić sygnał
- Samochód zignoruje niepoprawny sygnał
- My przechwytujemy wysłany sygnał
- Właściciel naciska ponownie

ILE TO KOSZTUJE?

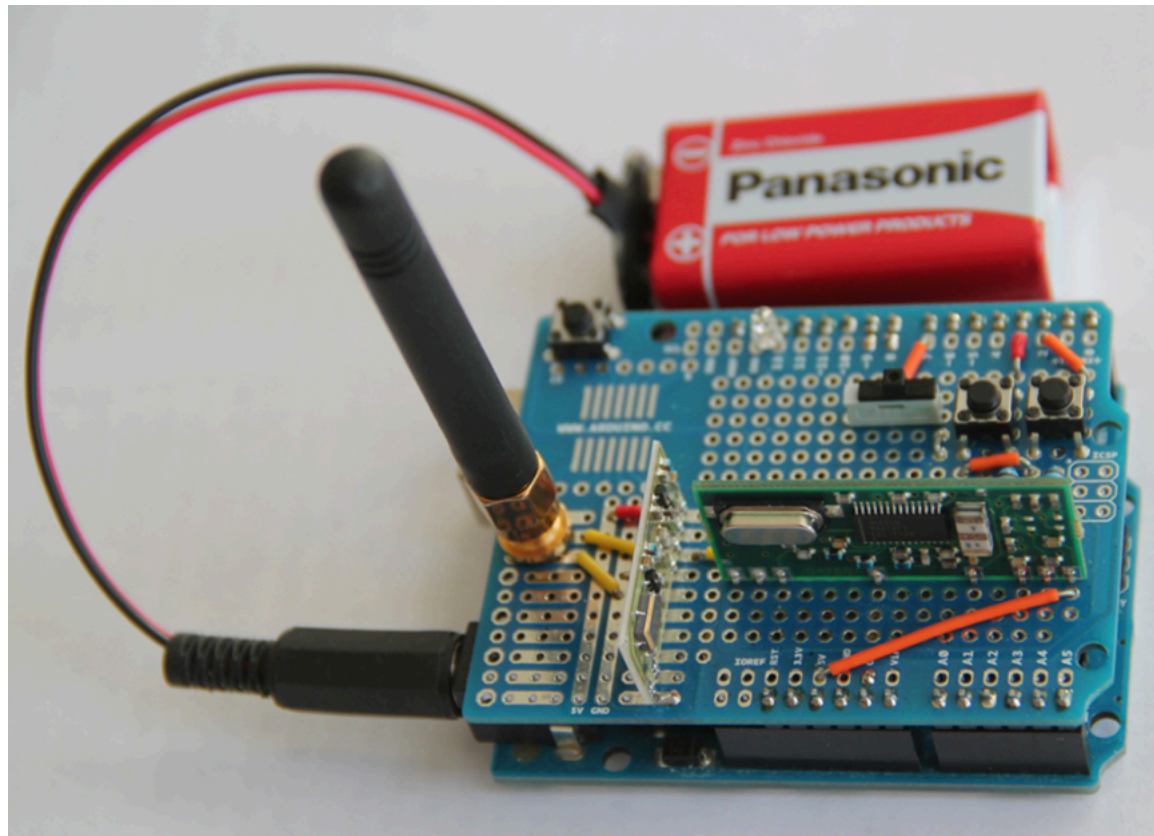


ILE TO KOSZTUJE?

.....



ILE TO KOSZTUJE?

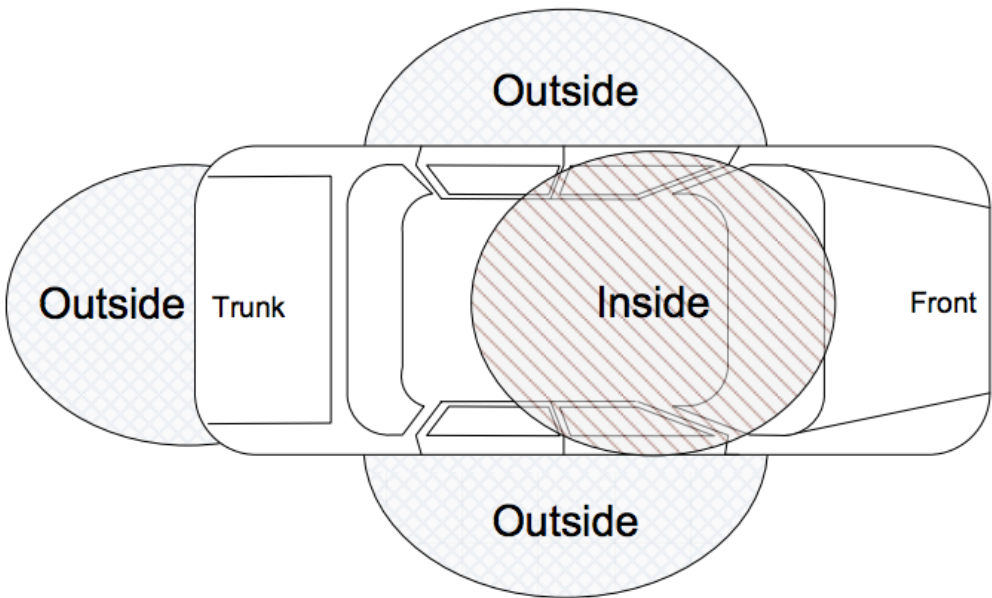


PKES

- PKES - Passive keyless entry and start
- Jeśli podejdziemy wystarczająco blisko samochód sam się otworzy
- Zagrożenie - Ataki typu przekaźnikowego

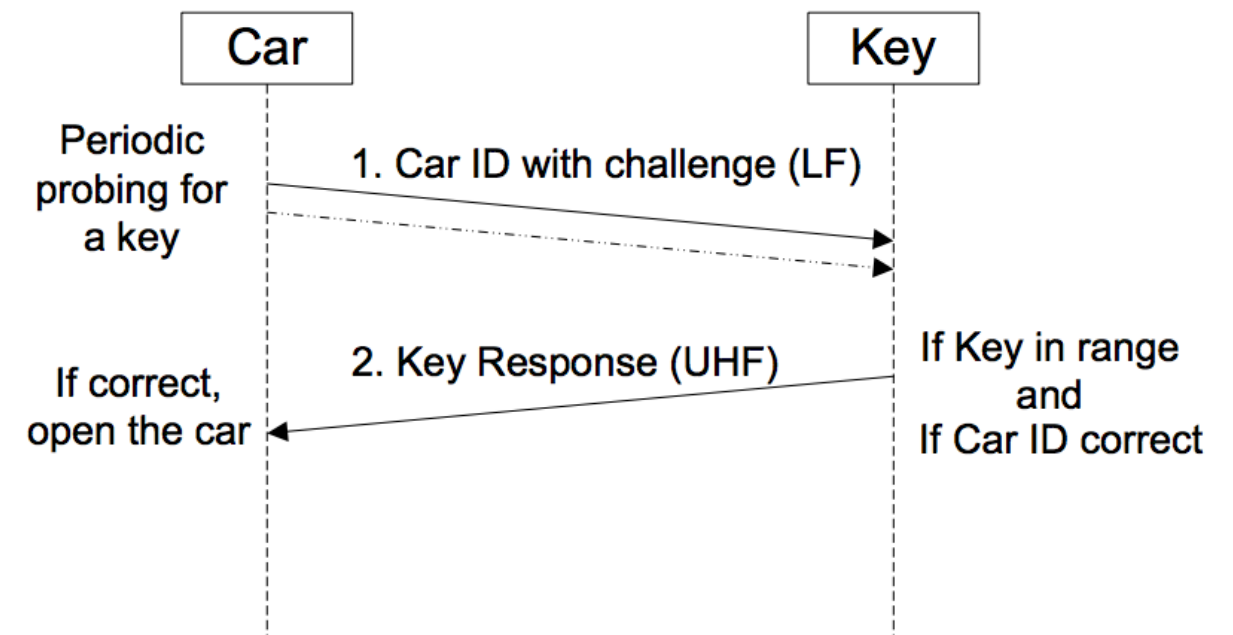
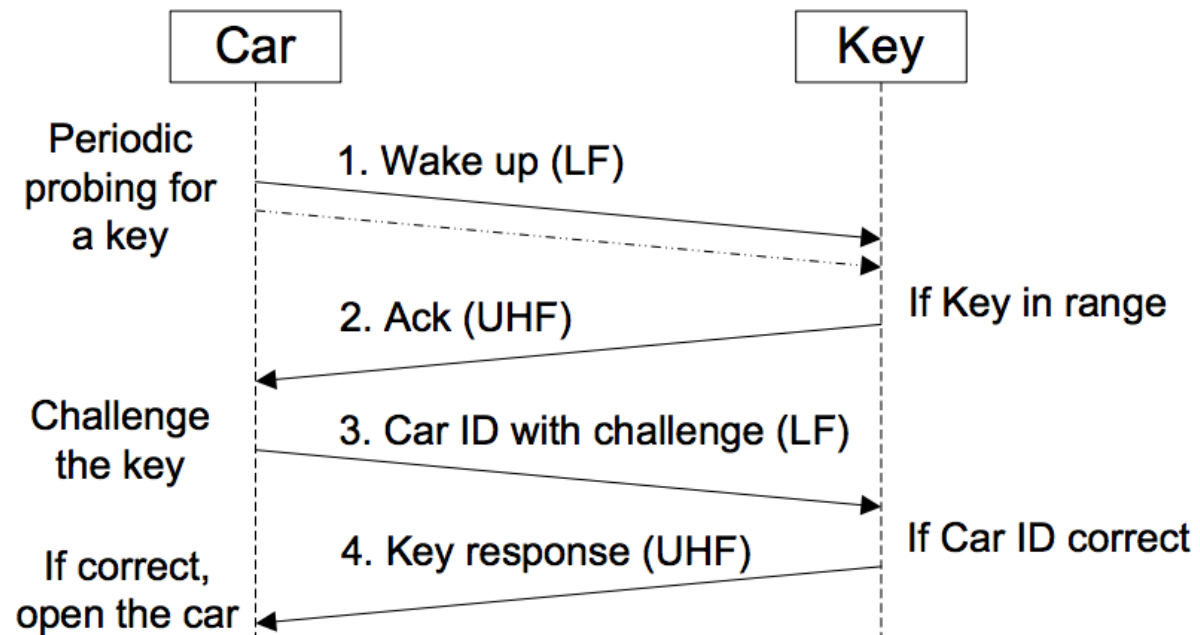
ZAKRESY DZIAŁANIA

.....

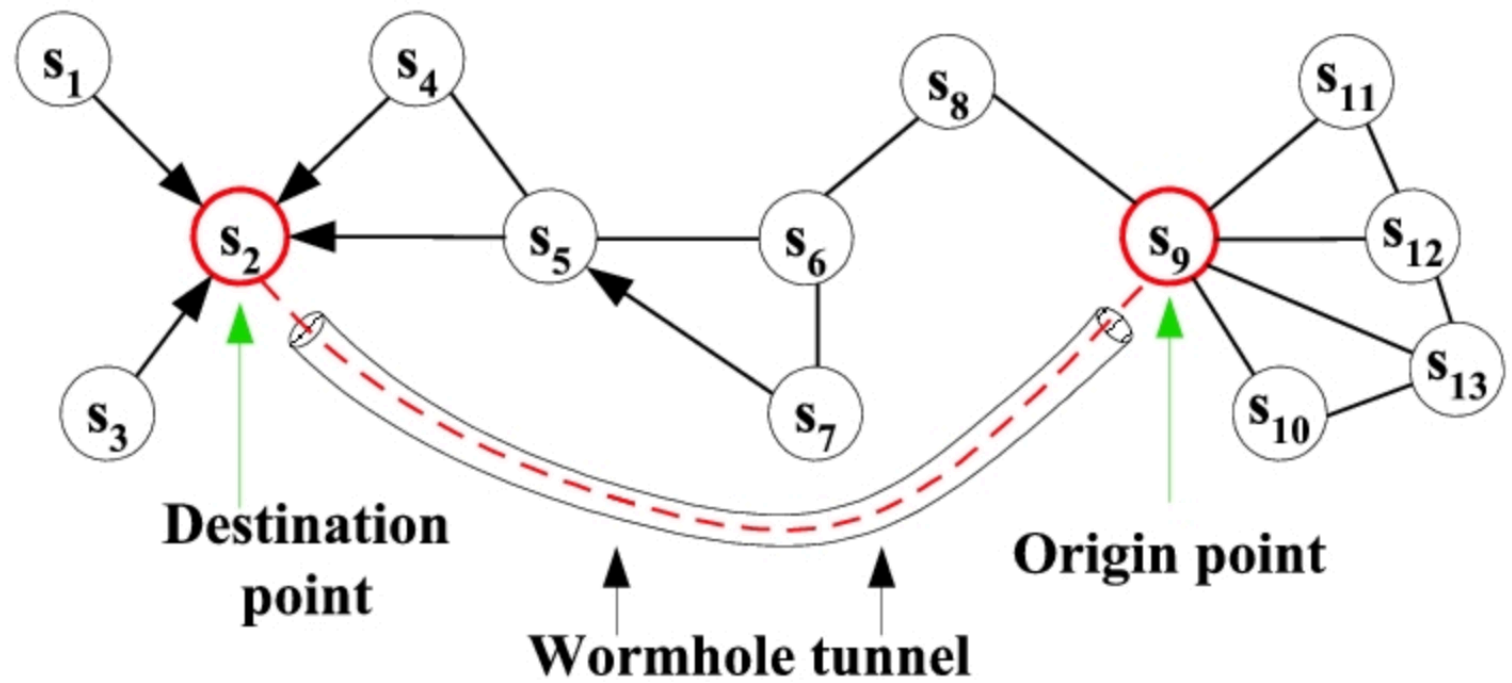


Key position	Authorization	Medium used	
		Car $\Rightarrow$ Key	Key $\Rightarrow$ Car
Normal mode: when the internal battery is present			
Remote	Active open/close	None	UHF
Outside	Passive open/close	LF	UHF
Inside	Passive start	LF	UHF
Backup mode: when the internal battery is exhausted			
Remote	Open/close	Impossible	
Outside	Open/close	With physical key	
Inside	Start	LF	LF

PROTOKOŁY PKES

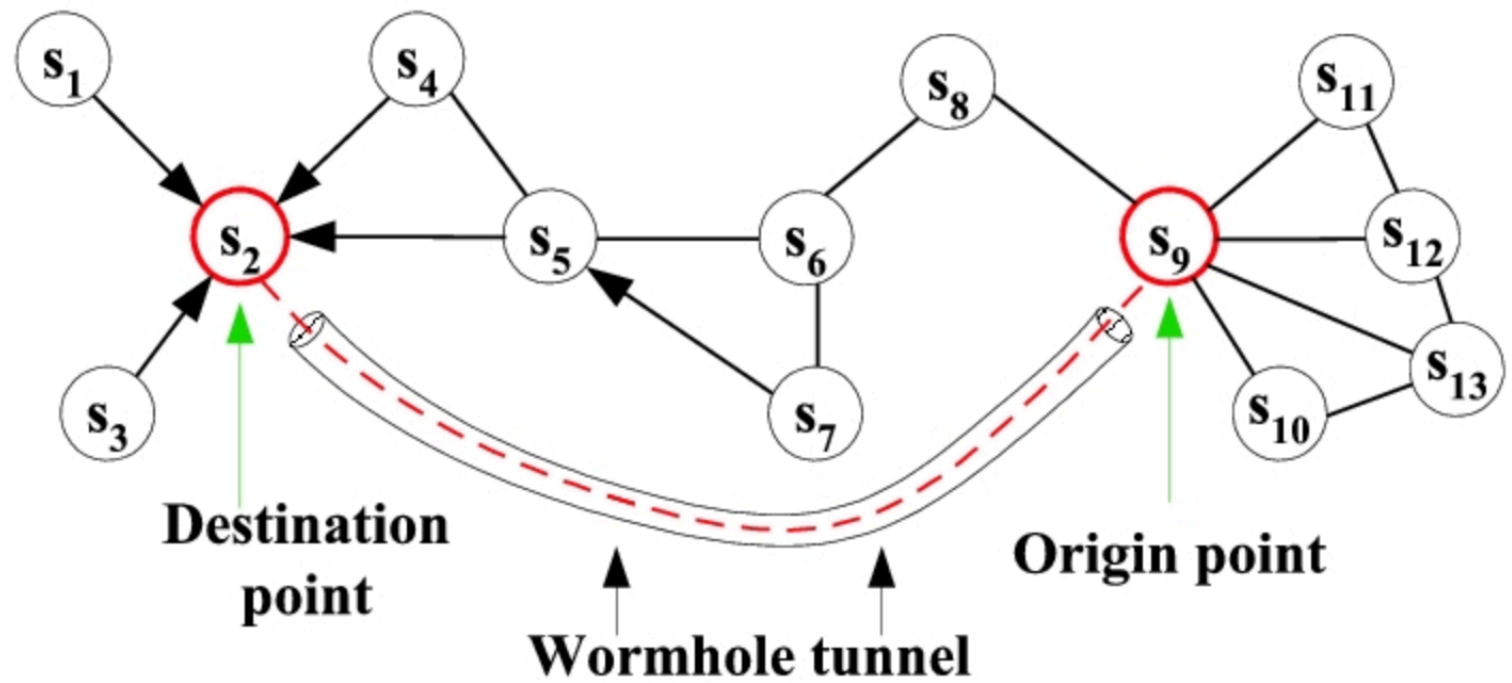


ATAK TYPU PRZEKAŹNIKOWEGO

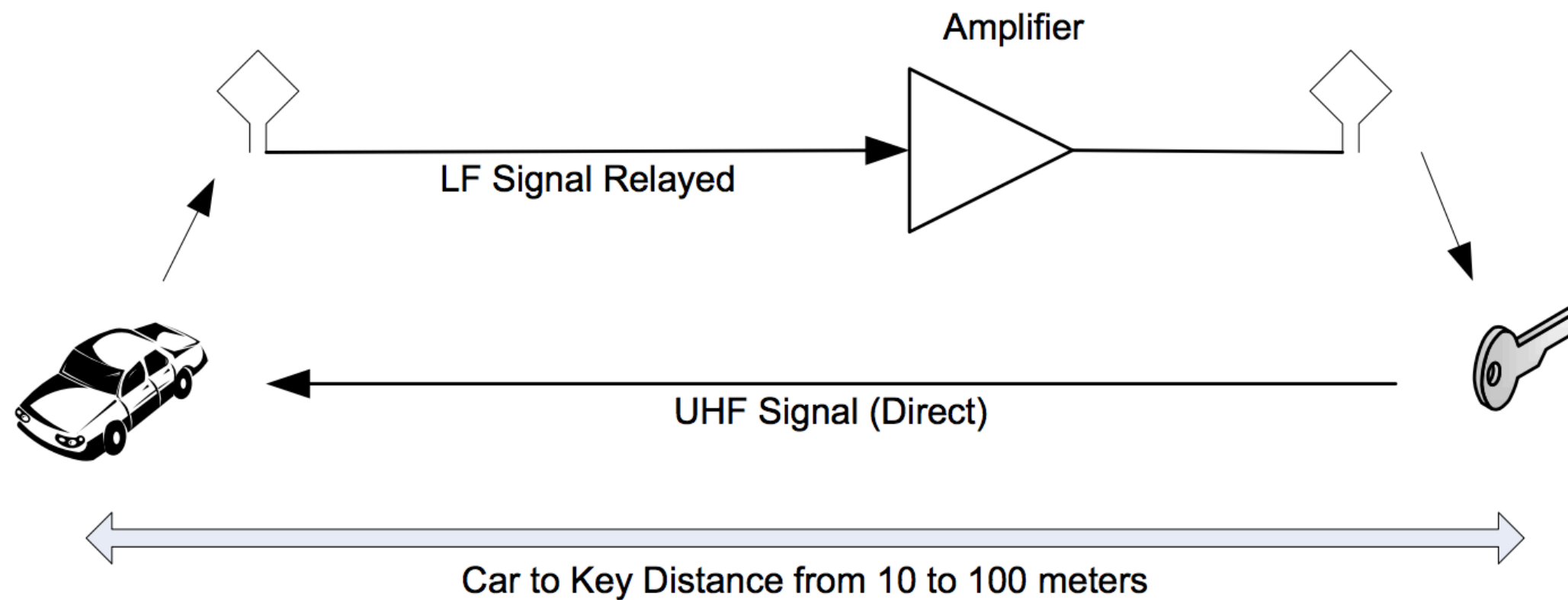


ATAK TYPU PRZEKAŹNIKOWEGO

.....

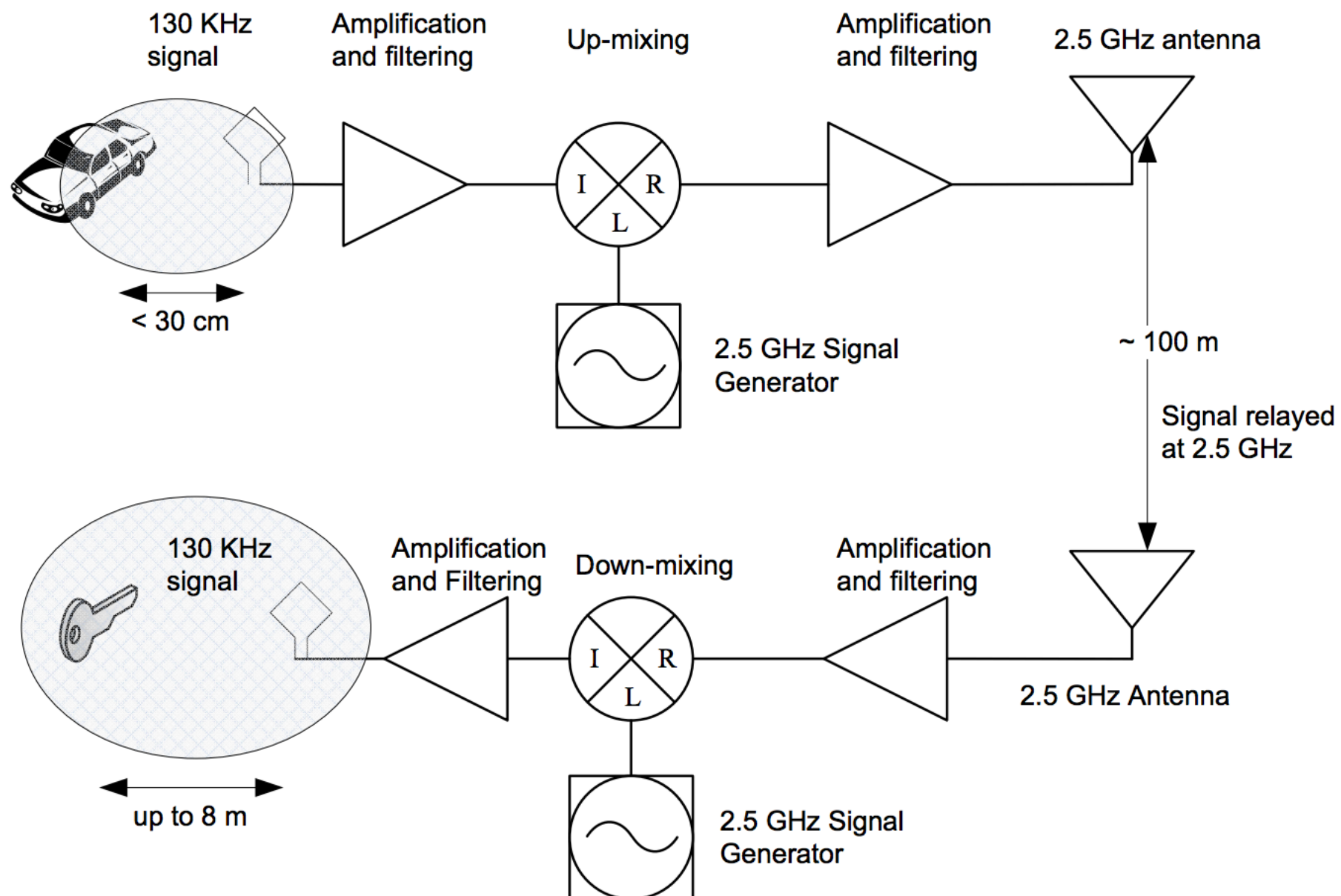


RELAY OVER-CABLE ATTACK



RELAY OVER-THE-AIR-ATTACK

.....



REZULTATY

Car model	Relay cable						Key to antenna distance (<i>m</i>)			
	7 <i>m</i>		30 <i>m</i>		60 <i>m</i>		No Amplifier		With Amplifier	
	open	go	open	go	open	go	open	go	open	go
Model 1	✓	✓	✓	✓	✓	✓	2	0.4	*	*
Model 2	✓	✓	A	A	A	A	0.1	0.1	2.4	2.4
Model 3	✓	✓	✓	✓	✓	✓	-	-	-	-
Model 4	✓	✓	-	-	-	-	-	-	-	-
Model 5	✓	✓	✓	✓	✓	✓	2.5	1.5	6	5.5
Model 6	✓	✓	A	A	A	A	0.6	0.2	3.5	3.5
Model 7	✓	✓	A	A	-	-	0.1	0.1	6	6
Model 8	✓	A	✓	A	-	-	1.5	0.2	4	3.5
Model 9	✓	✓	✓	✓	✓	✓	2.4	2.4	8	8
Model 10	✓	✓	✓	✓	-	-	-	-	-	-

PRZECIWDZIAŁANIA

Dla użytkownika:

Dla producenta

PRZECIWDZIAŁANIA

Dla użytkownika:

➤ Klatka Faradaya

Dla producenta

PRZECIWDZIAŁANIA

Dla użytkownika:

- Klatka Faradaya
- Wyjąć baterię

Dla producenta

PRZECIWDZIAŁANIA

Dla użytkownika:

- Klatka Faradaya
- Wyjąć baterię

Dla producenta

- Możliwość chwilowego wyłączenia PKES

PRZECIWDZIAŁANIA

Dla użytkownika:

- Klatka Faradaya
- Wyjąć baterię

Dla producenta

- Możliwość chwilowego wyłączenia PKES
- Zatrzymanie sygnału chwilę po otwarciu drzwi

PRZECIWDZIAŁANIA

Dla użytkownika:

- Klatka Faradaya
- Wyjąć baterię

Dla producenta

- Możliwość chwilowego wyłączenia PKES
- Zatrzymanie sygnału chwilę po otwarciu drzwi
- Hardare'owa wersja wyciągnięcia baterii



BIBLIOGRAFIA

- Aurelien Francillon, Boris Danev, Srdjan Capkun “Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars”
- Flavio D. Garcia, David Oswald, Timo Kasper, Pierre Pavlidès “Lock It and Still Lose It - On the (In)Security of Automotive Remote KeyLess Entry System”
- <https://en.wikipedia.org>
- Materiały ze studiów

PYTANIA ?