Gone in 360 Seconds: Hijacking with Hitag2

Roel Verdult **Flavio D. Garcia**

Radboud University Nijmegen,
The Netherlands

Josep Balasch

KU Leuven ESAT/COSIC
and IBBT, Belgium

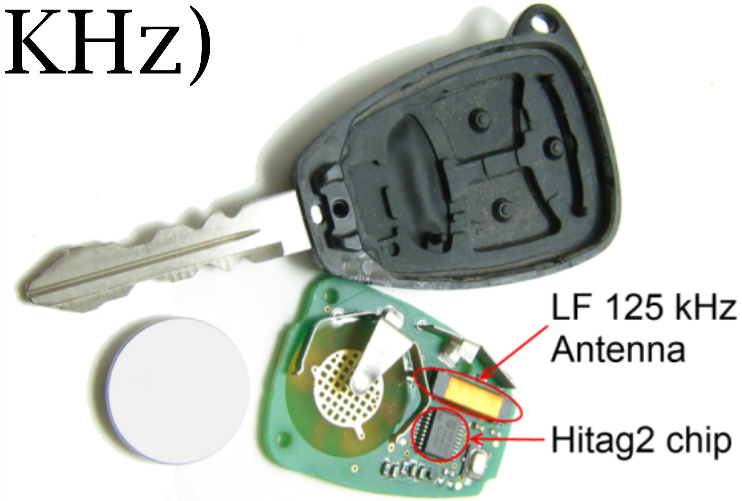
Institute for Computing and Information Sciences
Radboud University Nijmegen, The Netherlands
✉*rverdult@cs.ru.nl* *www.cs.ru.nl/~rverdult*

Contents

- Introduction
  - Vehicle Immobilizers
  - Hitag2 and its Usage
- Hitag2
  - Functionality
  - Cipher and Protocols Weaknesses
  - Attacks and Complexity
  - Practical Experiments
  - Mitigating Measures
- Conclusion

Vehicle Immobilizers

- Passive RFID Tag (125 KHz)
- Introduced in the '90s
- Prevents hot-wiring
- Mandatory
  - Europe (EU Directive 95/56/EC)
  - Australia (AS/NZS 4601:1999)
  - Canada (CAN/ULC S338- 98)

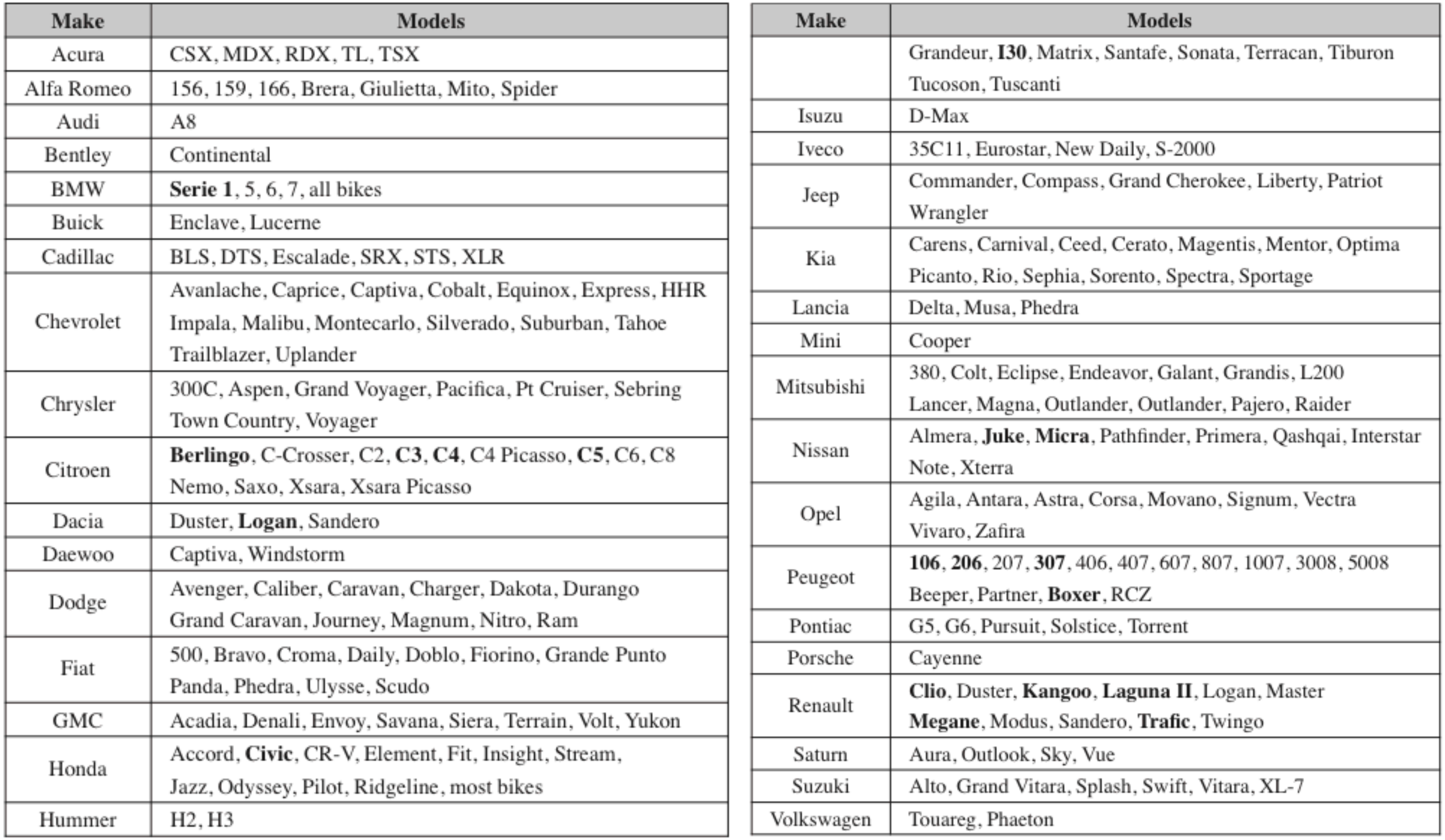


- Do **not** confuse it with remote controls that unlock the car doors (433 MHz)

Hitag2 Usage

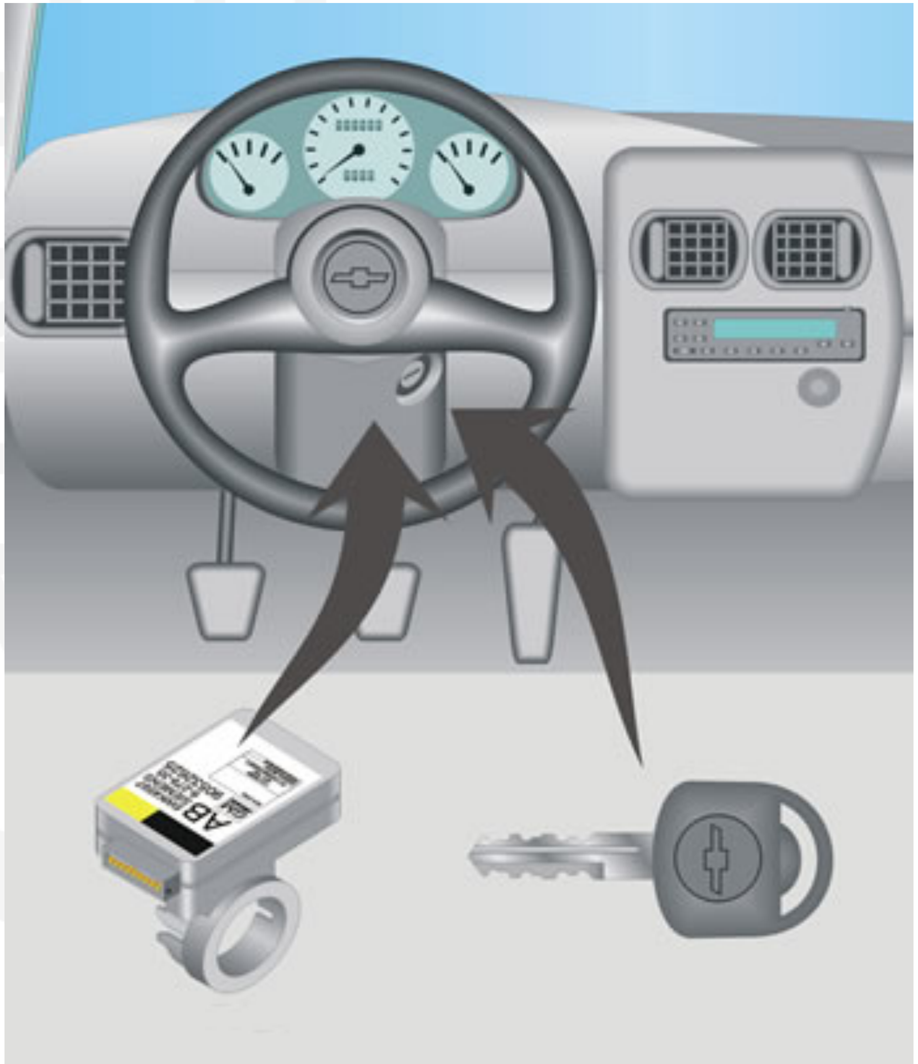
BMW
ACURA
GMC
NISSAN
KIA
ALFA ROMEO

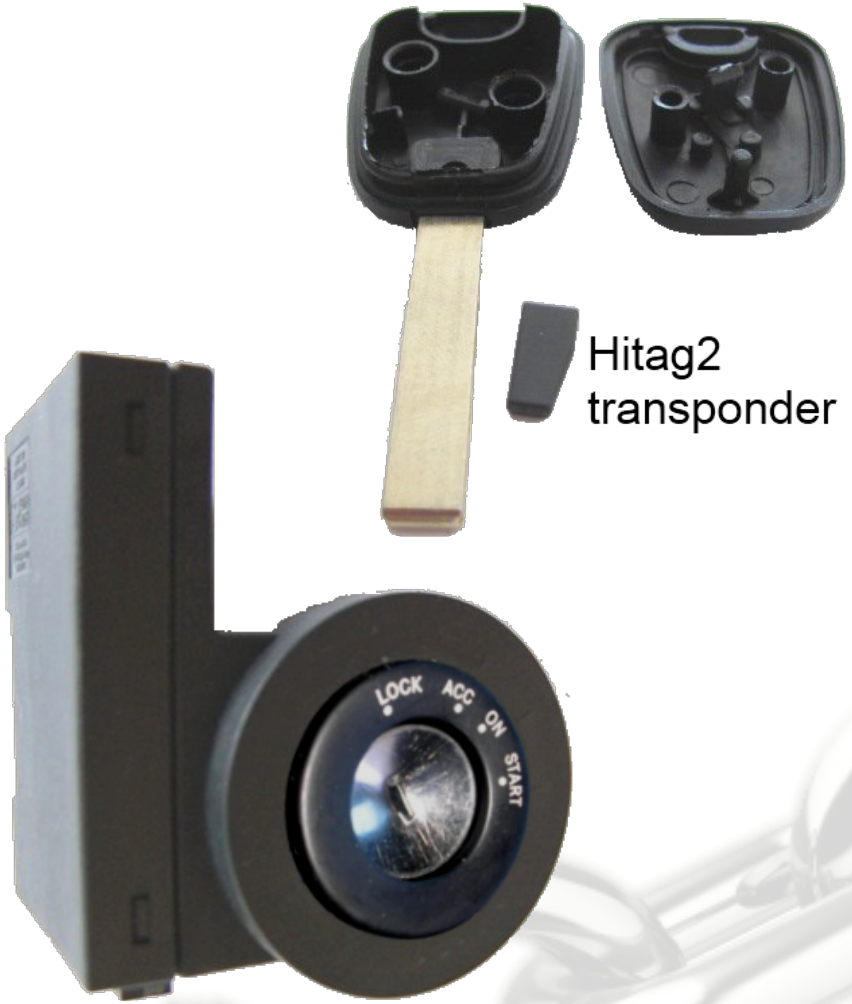
Makes & Models



Make	Models
Acura	CSX, MDX, RDX, TL, TSX
Alfa Romeo	156, 159, 166, Brera, Giulietta, Mito, Spider
Audi	A8
Bentley	Continental
BMW	**Serie 1**, 5, 6, 7, all bikes
Buick	Enclave, Lucerne
Cadillac	BLS, DTS, Escalade, SRX, STS, XLR
Chevrolet	Avanlache, Caprice, Captiva, Cobalt, Equinox, Express, HHR Impala, Malibu, Montecarlo, Silverado, Suburban, Tahoe Trailblazer, Uplander
Chrysler	300C, Aspen, Grand Voyager, Pacifica, Pt Cruiser, Sebring Town Country, Voyager
Citroen	**Berlingo**, C-Crosser, C2, **C3**, **C4**, C4 Picasso, **C5**, C6, C8 Nemo, Saxo, Xsara, Xsara Picasso
Dacia	Duster, **Logan**, Sandero
Daewoo	Captiva, Windstorm
Dodge	Avenger, Caliber, Caravan, Charger, Dakota, Durango Grand Caravan, Journey, Magnum, Nitro, Ram
Fiat	500, Bravo, Croma, Daily, Doblo, Fiorino, Grande Punto Panda, Phedra, Ulysse, Scudo
GMC	Acadia, Denali, Envoy, Savana, Siera, Terrain, Volt, Yukon
Honda	Accord, **Civic**, CR-V, Element, Fit, Insight, Stream, Jazz, Odyssey, Pilot, Ridgeline, most bikes
Hummer	H2, H3
	Grandeur, **I30**, Matrix, Santafe, Sonata, Terracan, Tiburon Tucoson, Tuscanti
Isuzu	D-Max
Iveco	35C11, Eurostar, New Daily, S-2000
Jeep	Commander, Compass, Grand Cherokee, Liberty, Patriot Wrangler
Kia	Carens, Carnival, Ceed, Cerato, Magentis, Mentor, Optima Picanto, Rio, Sephia, Sorento, Spectra, Sportage
Lancia	Delta, Musa, Phedra
Mini	Cooper
Mitsubishi	380, Colt, Eclipse, Endeavor, Galant, Grandis, L200 Lancer, Magna, Outlander, Outlander, Pajero, Raider
Nissan	Almera, **Juke**, **Micra**, Pathfinder, Primera, Qashqai, Interstar Note, Xterra
Opel	Agila, Antara, Astra, Corsa, Movano, Signum, Vectra Vivaro, Zafira
Peugeot	**106**, **206**, 207, **307**, 406, 407, 607, 807, 1007, 3008, 5008 Beeper, Partner, **Boxer**, RCZ
Pontiac	G5, G6, Pursuit, Solstice, Torrent
Porsche	Cayenne
Renault	**Clio**, Duster, **Kangoo**, **Laguna II**, Logan, Master **Megane**, Modus, Sandero, **Trafic**, Twingo
Saturn	Aura, Outlook, Sky, Vue
Suzuki	Alto, Grand Vitara, Splash, Swift, Vitara, XL-7
Volkswagen	Touareg, Phaeton

Vehicle Immobilizer

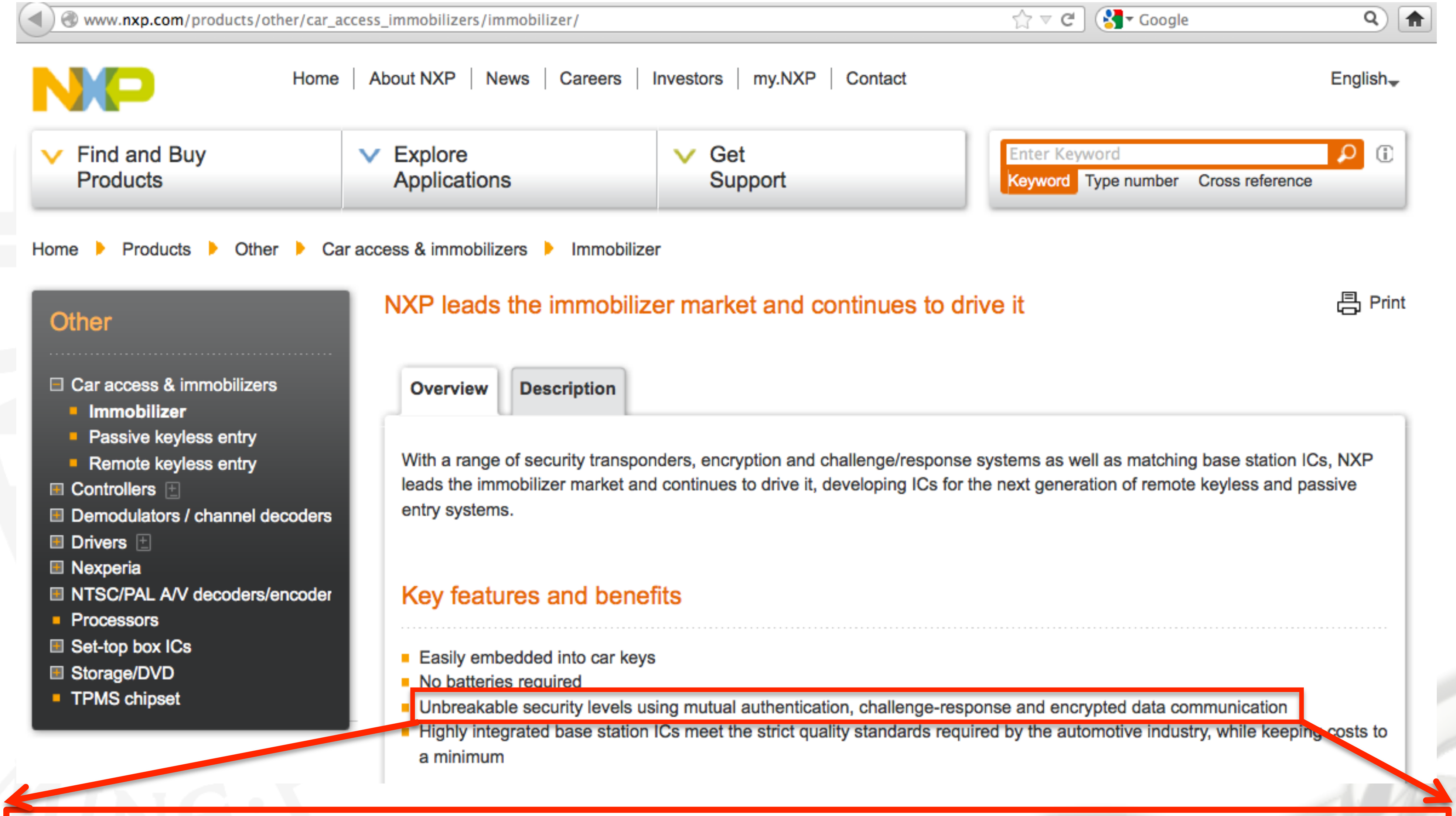




Hitag2 transponder

Hitag2 Functionality

- “Quotes” from the datasheet
  - Ideally suited for vehicle immobilization
  - Proximity (20cm) and long range (1m)
  - Effective communication protocol with outstanding data integrity check
  - Secret Key and a random number in order to cipher any communication
  - Mutual authentication function
  - To achieve a main stream security, data may be transmitted enciphered



NXP leads the immobilizer market and continues to drive it

With a range of security transponders, encryption and challenge/response systems as well as matching base station ICs, NXP leads the immobilizer market and continues to drive it, developing ICs for the next generation of remote keyless and passive entry systems.

Key features and benefits

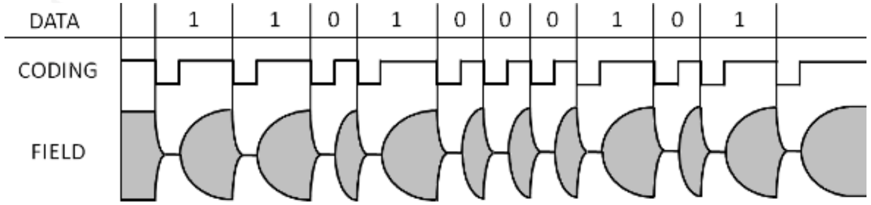
- Easily embedded into car keys
- No batteries required
- Unbreakable security levels using mutual authentication, challenge-response and encrypted data communication
- Highly integrated base station ICs meet the strict quality standards required by the automotive industry, while keeping costs to a minimum

Unbreakable security levels using mutual authentication, challenge-response and encrypted data communication

Hitag2 Functionality

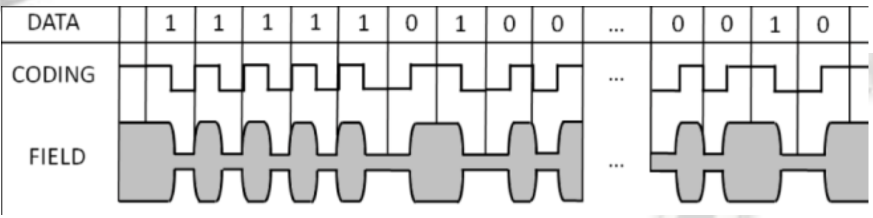
Block	Contents
0	transponder identifier *id*
1	secret key low $k_0 \ldots k_{31}$
2	secret key high $k_{32} \ldots k_{47}$ — reserved
3	configuration — password
4 – 7	user defined memory

Command	Bits
authenticate	11000
read	$11 n_0 n_1 n_2 00 \overline{n_0 n_1 n_2} \ldots$
$\overline{\textit{read}}$	$01 n_0 n_1 n_2 10 \overline{n_0 n_1 n_2} \ldots$
write	$10 n_0 n_1 n_2 01 \overline{n_0 n_1 n_2} \ldots$
halt	$00 n_0 n_1 n_2 11 \overline{n_0 n_1 n_2} \ldots$

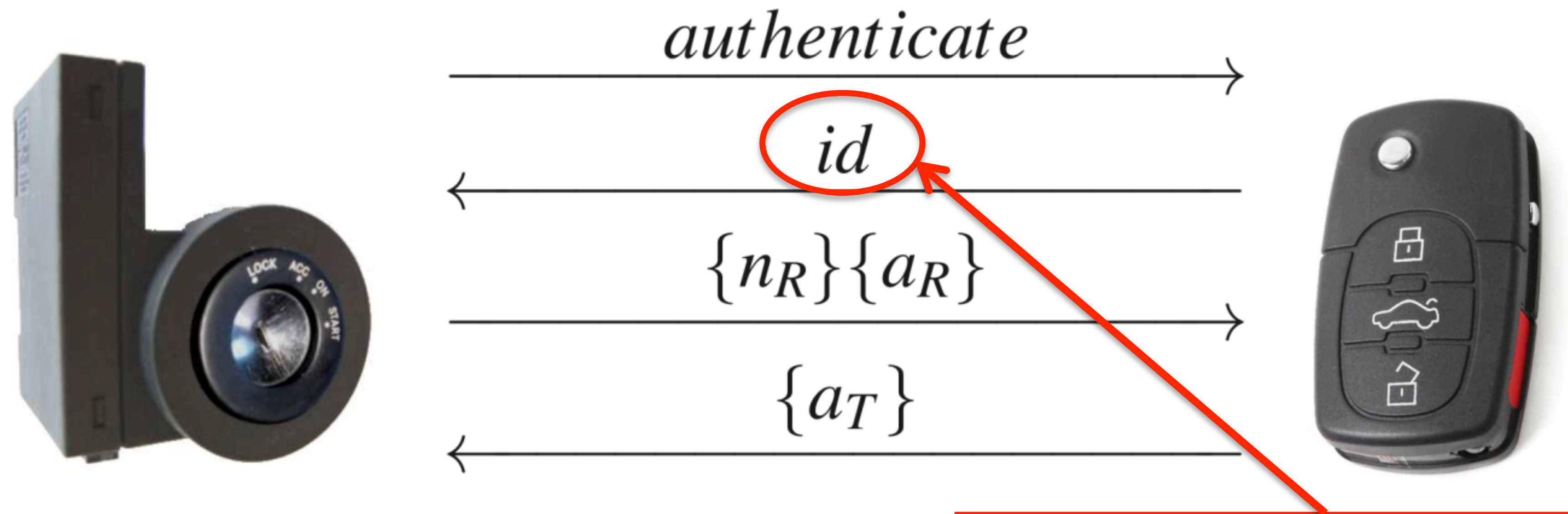


$\{11000001111100000111\}$ →

← $11111\{id_0 \ldots id_{31}\}$



Authentication Protocol



id = 32-bit identifier

{nR} = Encrypted reader nonce

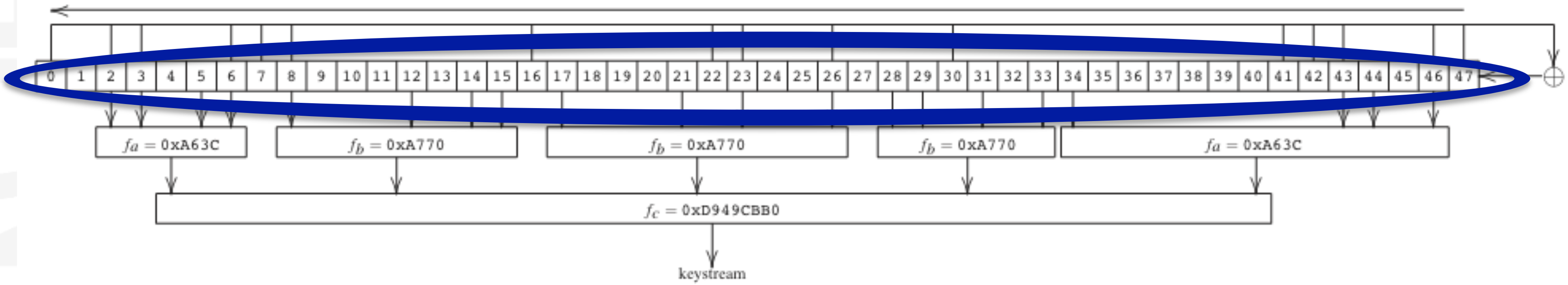
{aR} = Encrypted reader answer

{aT} = Encrypted tag answer

No tag nonce (nT)

Replay {nR}{aR} results in same keystream

Hitag2 Cipher



- **48 bit internal state (LFSR stream $a_0a_1\ldots$)**

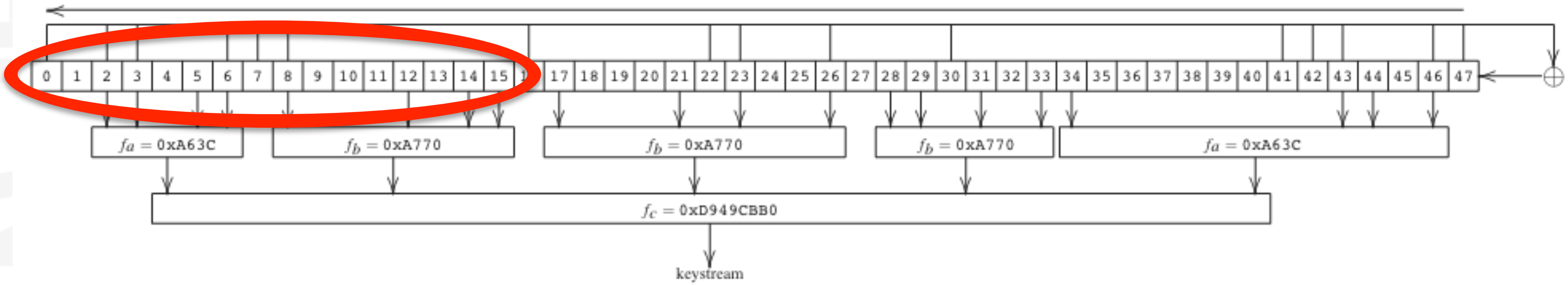
$a_0 \ldots a_{31} = id_0 \ldots id_{31}$

$a_{32} \ldots a_{47} = k_0 \ldots k_{15}$

$$a_{48+i} = k_{16+i} \oplus \{nr\}_i \oplus f(a_i \ldots a_{47+i})_i \quad \forall i \in [0,31]$$

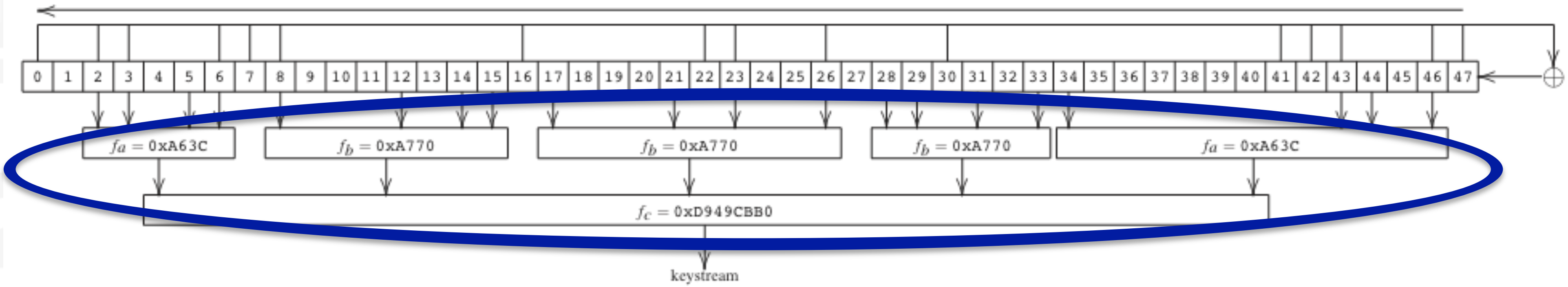
Initialized LFSR = $a_{32} \ldots a_{79}$

Hitag2 Cipher



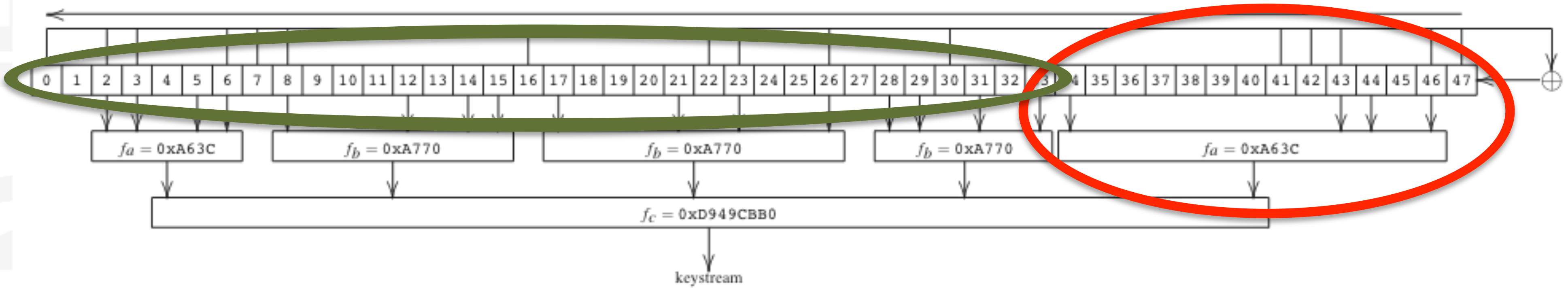
- Dependencies between sessions
  - Reader nonce (nR) is **only 32 bits**
  - Remember that $a_{32} \ldots a_{47} = k_0 \ldots k_{15}$ and initialized LFSR = $a_{32} \ldots a_{79}$
  - **We can conclude that $\text{LFSR}_0 \ldots \text{LFSR}_{15}$ are fixed for each session, regardless of nr**

Hitag2 Cipher



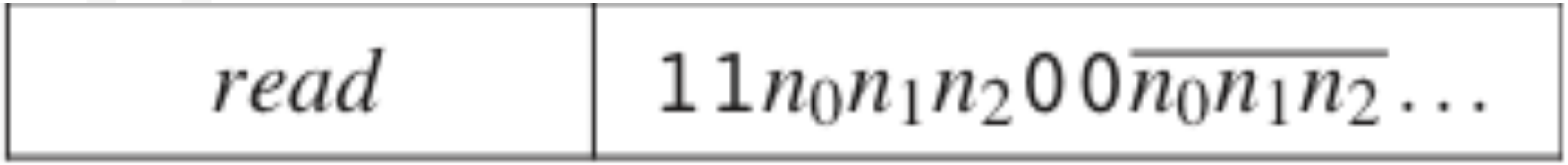
- **Non-linear filter function (20 → 1 bit)**
  - Contains sub-functions with fewer inputs
  - Tree function with two layers
  - There are 5 sub-functions with 4-bit input
  - Each function delivers one input bit for second layer function f_c

Hitag2 Cipher



- Filter function weakness
  - 4 bits cover 14 bits of the internal state
  - In 8 of the 32 configurations, the output of f_c is **not** influenced by the last bit
  - Probability ¼ the output is determined by the first 34 bits of the filter function

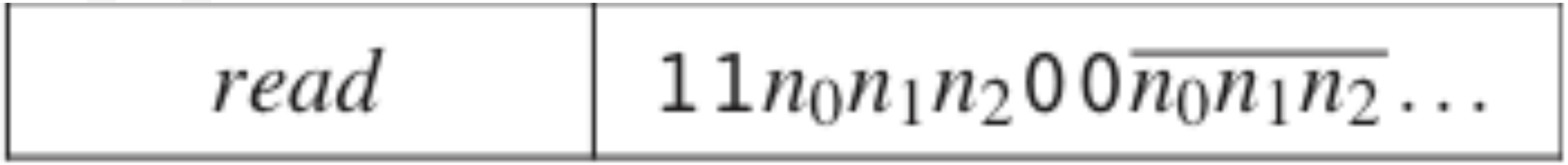
Hitag2 Protocol



read	$11n_0n_1n_2 00\overline{n_0n_1n_2}\ldots$

- After authentication, it uses encrypted instructions of 5 bits which are sent (at least) twice
- The instruction is concatenated with its complement for integrity
- Extra redundancy can be achieved by adding complements multiple times

Hitag2 Protocol



read	$11n_0n_1n_2 00\overline{n_0n_1n_2}\ldots$

- Instruction contains a 2-bit command and a 3-bit memory block
- Some examples of (equivalent) read instructions on memory block 3
  - *read* (block3) = 11011 00100
  - *read* (block3) = 11011 00100 11011
  - *read* (block3) = 11011 00100 11011 00100

Hitag2 Protocol

- **Replay** same {nR}{aR} and use variable length to get a keystream oracle

$$\begin{array}{rl} \text{read (block3)} = & 11011\ \ 00100 \\ \text{keystream} = & \underline{01010\ \ 01101 \oplus} \\ & 10001\ \ 01001 \end{array}$$

Try all 32 possibilities, only answers when correct

$$\begin{array}{rl} \text{read (block3)} = & 11011\ \ 00100\ \ 11011 \\ \text{keystream} = & \underline{01010\ \ 01101\ \ ..... \oplus} \\ & 10001\ \ 01001\ \ ..... \end{array}$$

Malleability attack

- Eavesdrop **only one** authentication attempt {nR}{aR} from the car
- Use oracle to recover 42 of keystream bits, enough to read out the memory
- Recover all memory blocks except the secret key (could be read protected)
  - If not configured correctly, the secret key is still readable.
  - **In such a case the total attack time is less than one second**

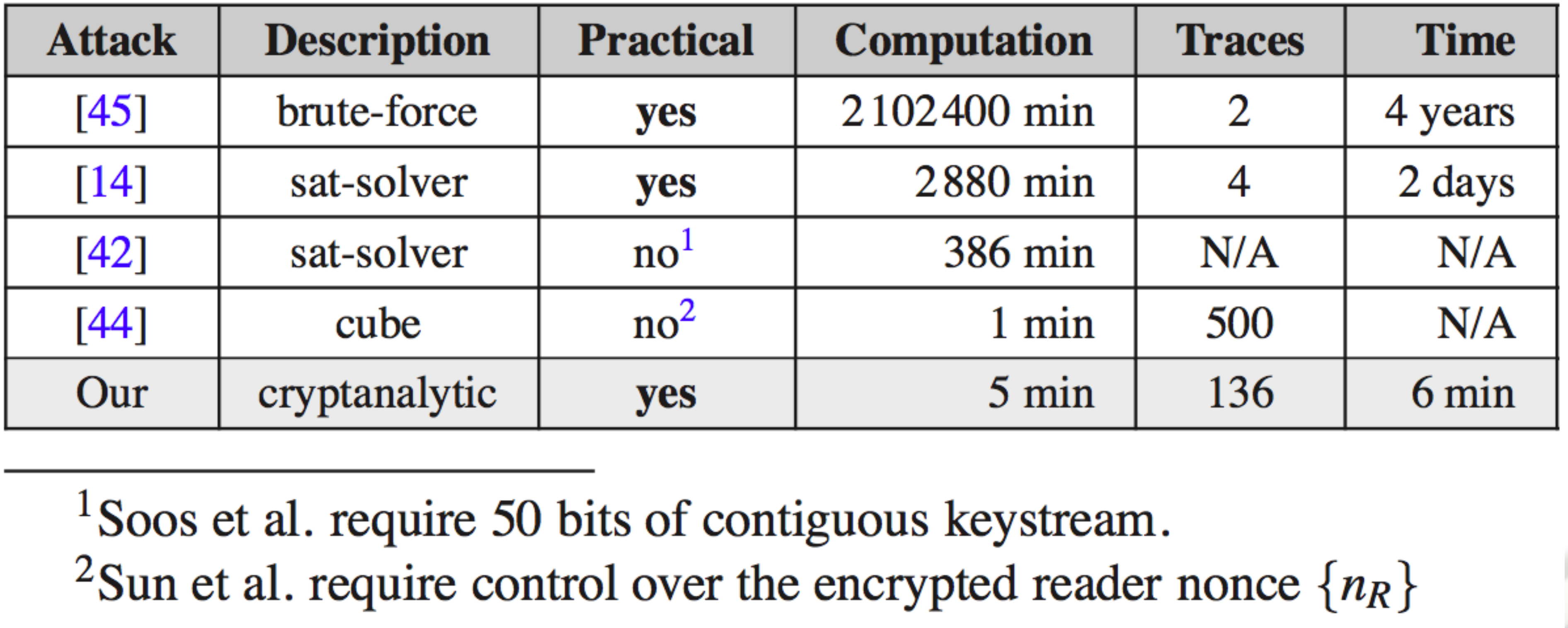
Time/memory tradeoff attack

- Once, use a smart trick to build a table with 2^{37} cipher states
  - Sort table on 48 produced keystream bits
- Eavesdrop **only one** authentication attempt {nR}{aR} from the car
- Use keystream oracle to recover 2^{11} bits
- Apply sliding window on contiguous keystream and find table entry
- **Total attack time is one minute**

Cryptanalytic Attack

- Gather only 134 authentication attempts from the car **(~1 minute)**
- Use first cipher weakness to combine different reader nonces
- Try for every 2^{34} cipher state **(~5 minutes)**
  - Which ¼ of the 134 are useful to eliminate
  - If first keystream bit of {ar} passes the test
  - Verify handful of candidate keys
- **Total attack time is 360 seconds**

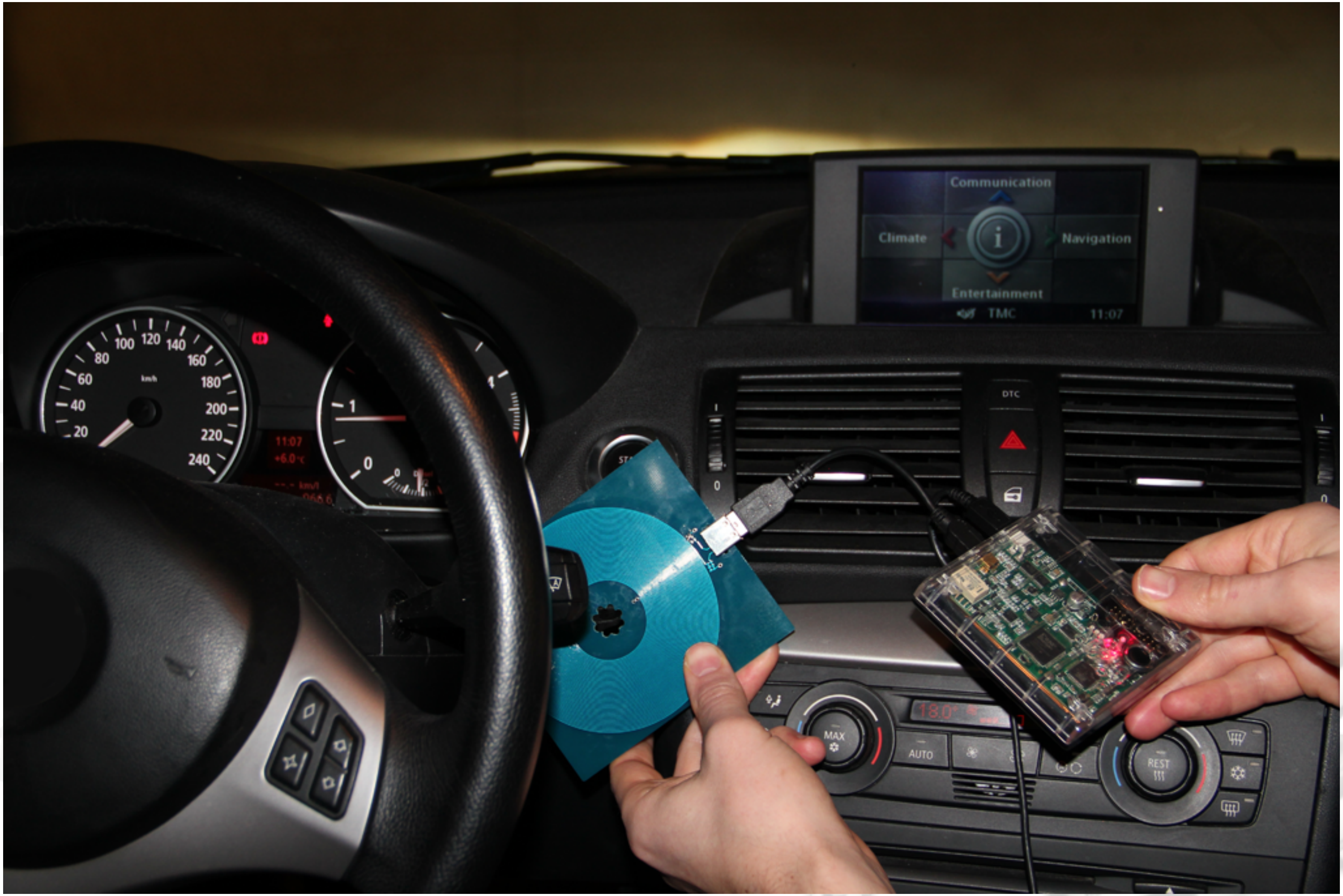
Comparison and Complexity



Attack	Description	Practical	Computation	Traces	Time
[45]	brute-force	**yes**	2 102 400 min	2	4 years
[14]	sat-solver	**yes**	2 880 min	4	2 days
[42]	sat-solver	no[1]	386 min	N/A	N/A
[44]	cube	no[2]	1 min	500	N/A
Our	cryptanalytic	**yes**	5 min	136	6 min

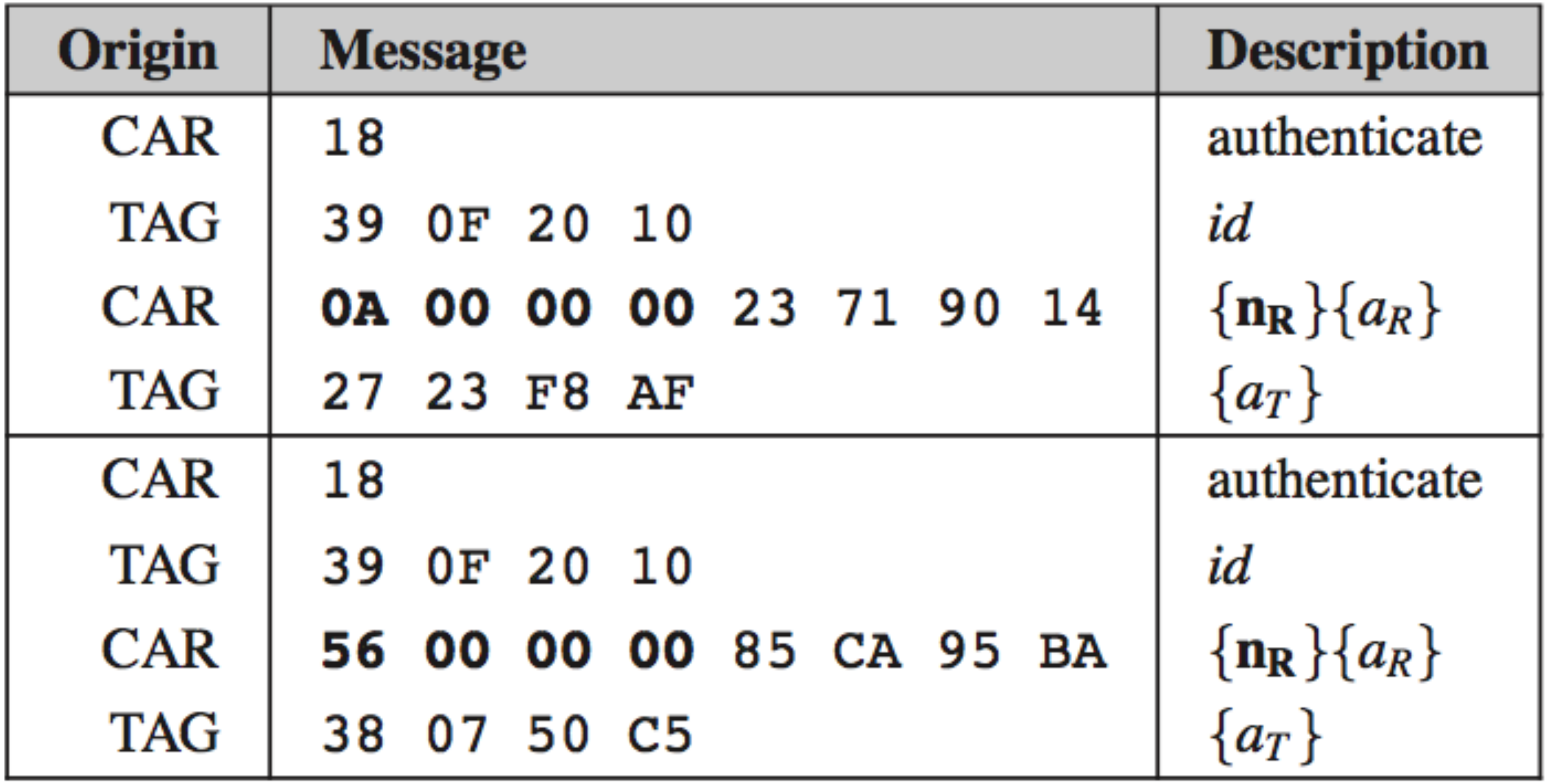
[1] Soos et al. require 50 bits of contiguous keystream.

[2] Sun et al. require control over the encrypted reader nonce $\{n_R\}$


Communication
Climate
Navigation
Entertainment
TMC
11:07
DTC
MAX
AUTO
REST

Practical Experiments

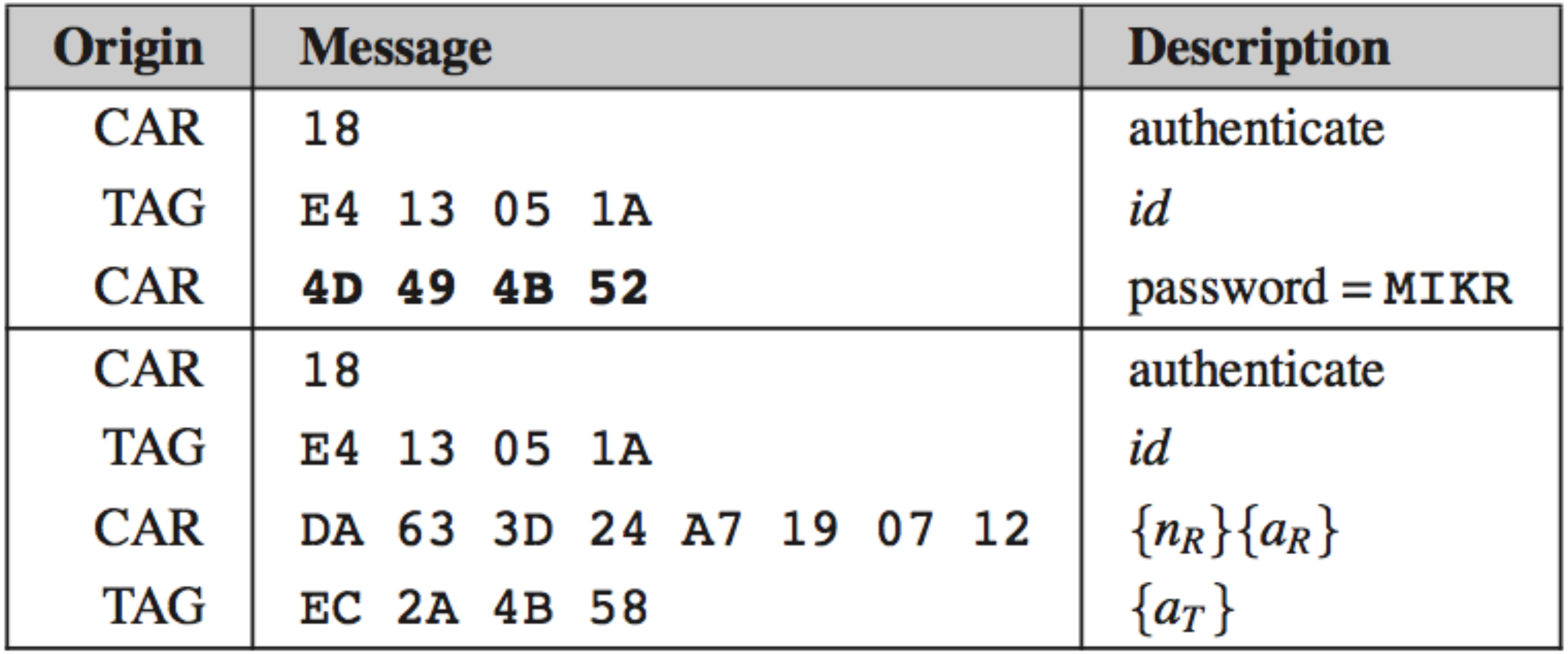
- Weak random number generators



Origin	Message	Description
CAR	18	authenticate
TAG	39 0F 20 10	*id*
CAR	**0A 00 00 00** 23 71 90 14	$\{\mathbf{n_R}\}\{a_R\}$
TAG	27 23 F8 AF	$\{a_T\}$
CAR	18	authenticate
TAG	39 0F 20 10	*id*
CAR	**56 00 00 00** 85 CA 95 BA	$\{\mathbf{n_R}\}\{a_R\}$
TAG	38 07 50 C5	$\{a_T\}$

Practical Experiments

- Weak authentication
  - – Default password “MIKR”
  - – Using key of the form 0xFFFF* * * * **FF

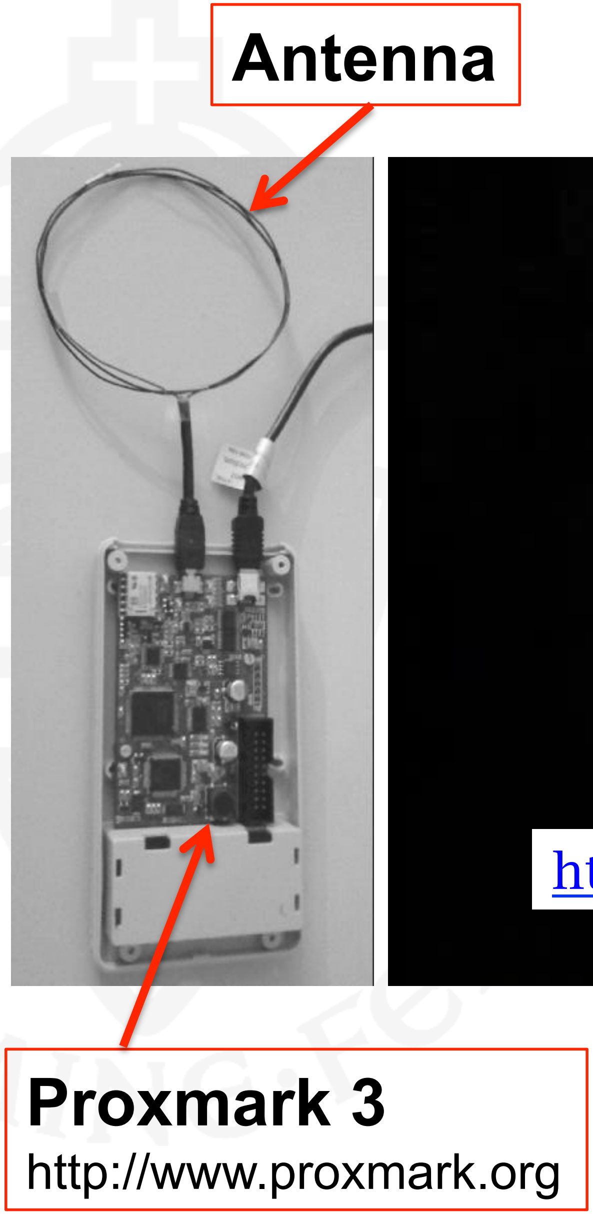


Origin	Message	Description
CAR	18	authenticate
TAG	E4 13 05 1A	*id*
CAR	**4D 49 4B 52**	password = MIKR
CAR	18	authenticate
TAG	E4 13 05 1A	*id*
CAR	DA 63 3D 24 A7 19 07 12	$\{n_R\}\{a_R\}$
TAG	EC 2A 4B 58	$\{a_T\}$

Practical Experiments

- Tested cars use identifier white-listing
  - Car stores a list of known keys (identifiers)
  - Only authenticates to known identifiers
- First wirelessly pickpocket this identifier
  - Low frequency 125 KHz
    - Few inches
    - Approach victim a few milliseconds
  - High frequency 433 MHz
    - Up to 300 feet
    - Eavesdrop when owner closes the doors

Wirelessly Pickpocketing



Antenna

Proxmark 3
http://www.proxmark.org

http://www.youtube.com/watch?v=UMPs1Zv8tDI

http://www.youtube.com/watch?v=S8z9mgIkqBA

- Starting BMW-1 engine
- Look at tachometer
- Without original key
- Using empty key shell and Proxmark to bypass the immobilizer
- Car keeps running after successful authentication

- Start and drive BMW-5
- Car costs $100,000 USD
- Broadcasted on the Dutch national television

http://www.youtube.com/watch?v=QomCiTjqJgo

Attack implications

- Cipher is broken beyond repair
- With tuned antenna larger pickpocket distances can be achieved
- Very serious when the attacker has a few seconds access to the car and key
  - While renting a car
  - Valet parking at hotel
  - Test drive at the dealer
  - Insurance fraud, car owner theft

Conclusion

- Security by obscurity often covers up negligent designs
- Immobilizer based on 3DES or AES cost only a few dollars more
- Notified the manufacturer NXP
  - Responsible disclosure (6 months ahead)
  - Verified and acknowledged our findings
  - Collaborated constructively by discussing mitigating measures