Breaking automotive remote keyless entry systems

or: why your car is not a safe box

David Oswald[1]

joint work with: Flavio D. Garcia[1], Timo Kasper[2] and Pierre Pavlidès[1]

1. University of Birmingham, UK
2. Kasper & Oswald GmbH, Germany

UNIVERSITY OF BIRMINGHAM

KASPER OSWALD
Innovative Security Engineering


PER ARDUA
AD ALTA
UNIVERSITY OF BIRMINGHAM
Google

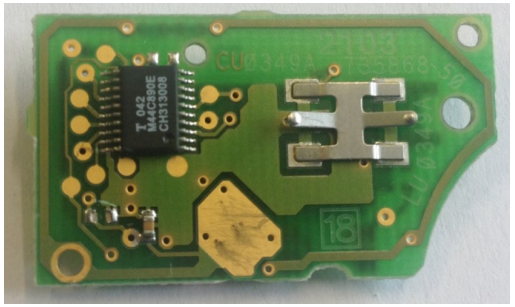
Immobilizer (Immo)

- Passive RFID at 125 kHz
- Many broken systems (DST40, Hitag2, Megamos)

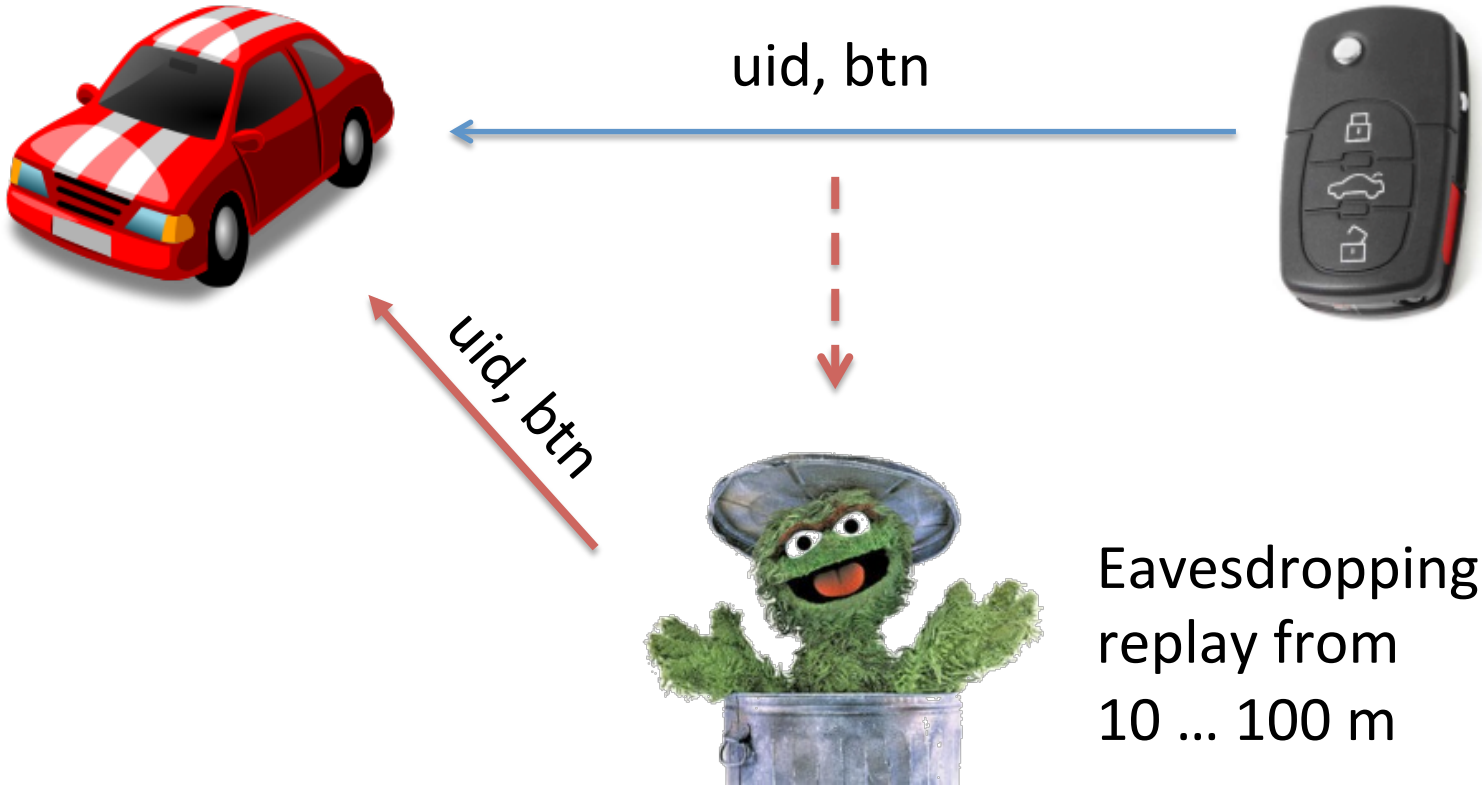
Wireless attacks?

Remote Keyless Entry (RKE)

- Active UHF transmitter (315 / 433 / 868 MHz)
- Unidirectional
- Sometimes integrated with immobilizer chip ("hard"), sometimes separate

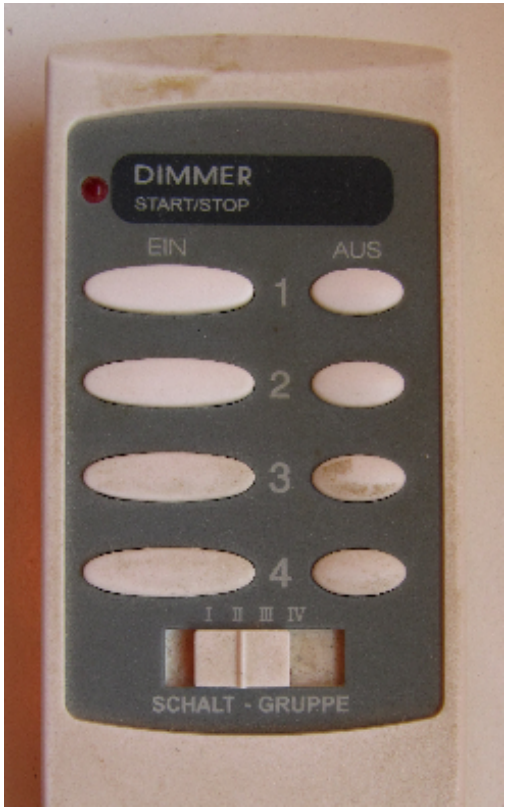


Fix codes



Eavesdropping and replay from 10 … 100 m

More examples for fix code systems



Rolling codes

uid, $enc_K(ctr', btn)$

uid, $enc_K(ctr' + 1, btn)$

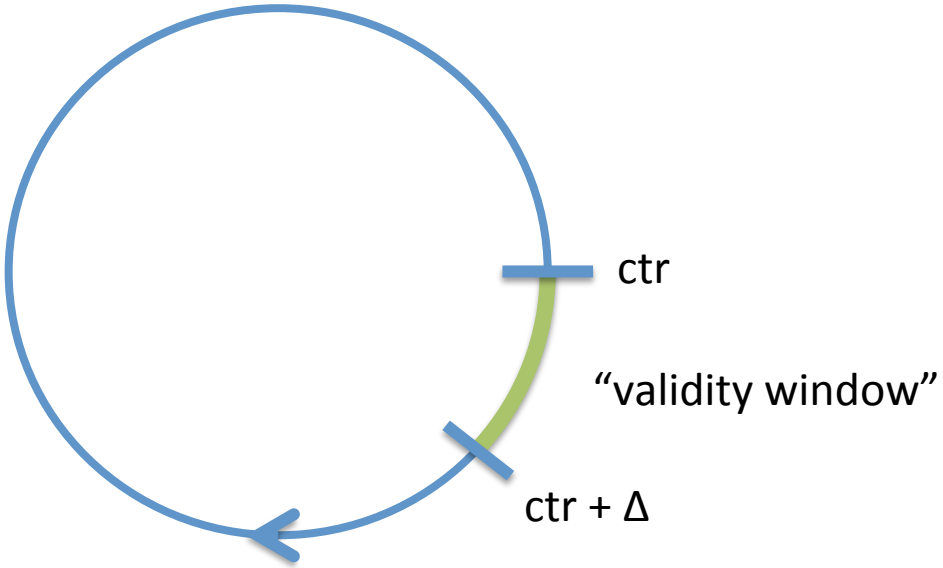
uid, $enc_K(ctr' + 2, btn)$

Decrypt ctr'

if (ctr < ctr' < ctr + Δ)

ctr := ctr'

open / close



Rolling codes

uid, $enc_K(ctr', btn)$

Note: there are some devices (medical) that use rolling codes w/o crypto

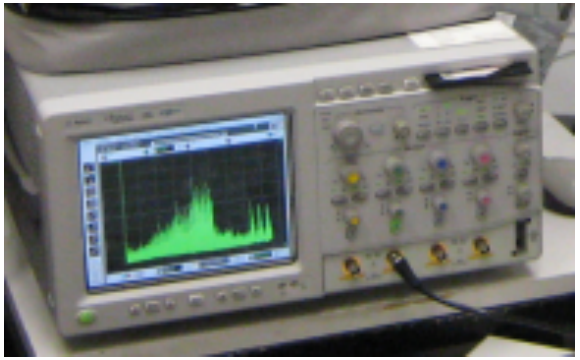
ctr' incremented on each button press, replay fails

Previous attacks on RKE

- 2007: Cryptanalysis of KeeLoq garage door openers (2^{16} plaintext/ciphertext pairs) by Biham et al.
- **2008: Side-channel attack on KeeLoq key diversification (Eisenbarth et al.)**

Side-channel attacks on KeeLoq

- Key derivation based on manufacturer key k_M: $k_{device} = f(uid, k_M)$
- Recover k_{device} with 10 power traces
- But: k_M used in every receiver of manufacturer
- Recover k_M with single power trace
- Single point of failure



Previous attacks on RKE

- 2007: Cryptanalysis of KeeLoq garage door openers (2^{16} plaintext/ciphertext pairs) by Biham et al.
- 2008: Side-channel attack on KeeLoq key diversification (Eisenbarth et al.)
- **2010: Relay attacks on passive keyless entry systems (Francillon et al.)**

Passive keyless entry systems (PKES)

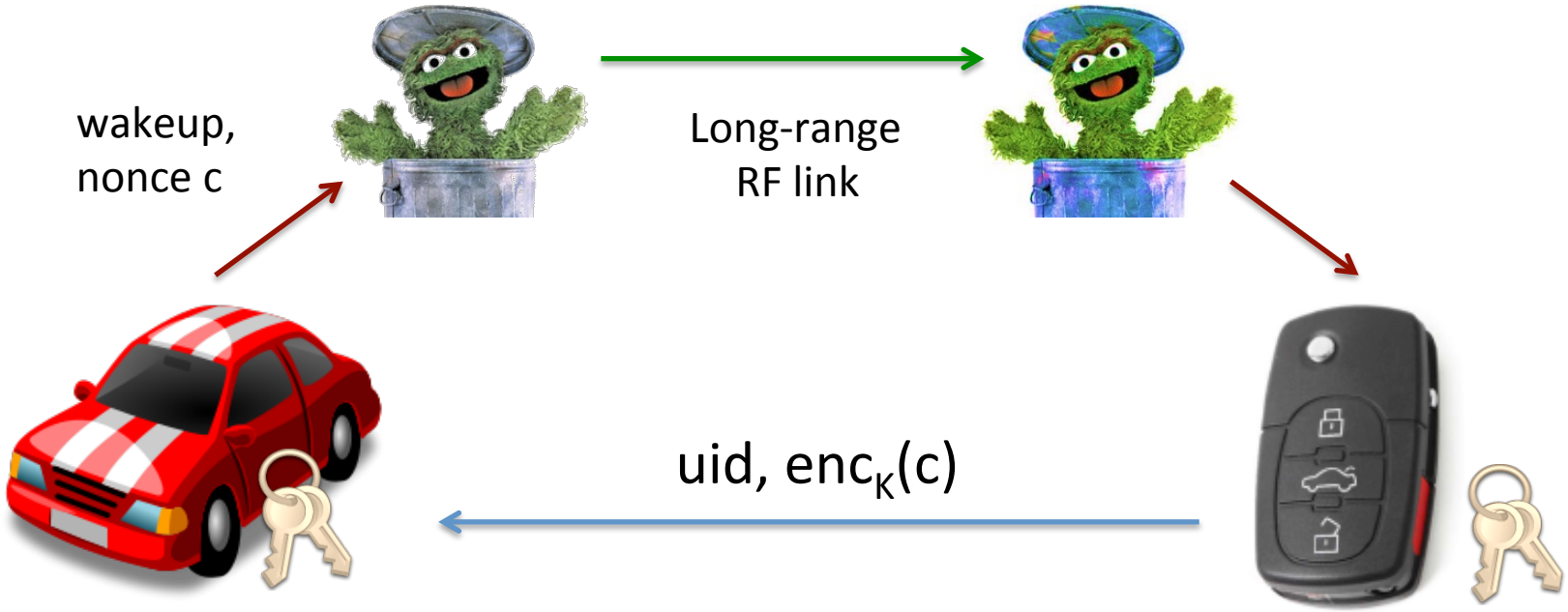
wakeup, nonce c

uid, $enc_K(c)$

Car to key: 125 kHz, short range

Key to car: 433 MHz, long range

Relay attacks on PKES



Car to key: 125 kHz, short range

Key to car: 433 MHz, long range

Montag, den 10.10.2016, 9:00 Uhr, Landgericht Detmold (Strafkammer I)

Strafsache gegen M. aus Litauen, Verteidigerin: Rechtsanwältin Grohmann aus Münster

wegen schweren Bandendiebstahls in 21 Fällen
Staatsanwaltschaft Detmold 31 Js 199/16

Die Staatsanwaltschaft Detmold legt dem 28 Jahre alten Angeklagten folgendes zur Last:

Der Angeklagte soll Mitglied einer organsiert agierenden Gruppe litauischer Autoschieber sein, die in Deutschland Fahrzeuge der Oberklasse mit einem Wert zwischen 33.000,00 und 130.000,00 € entwendet haben sollen, welche mit einem Keyless-Go-System ausgestattet sind.

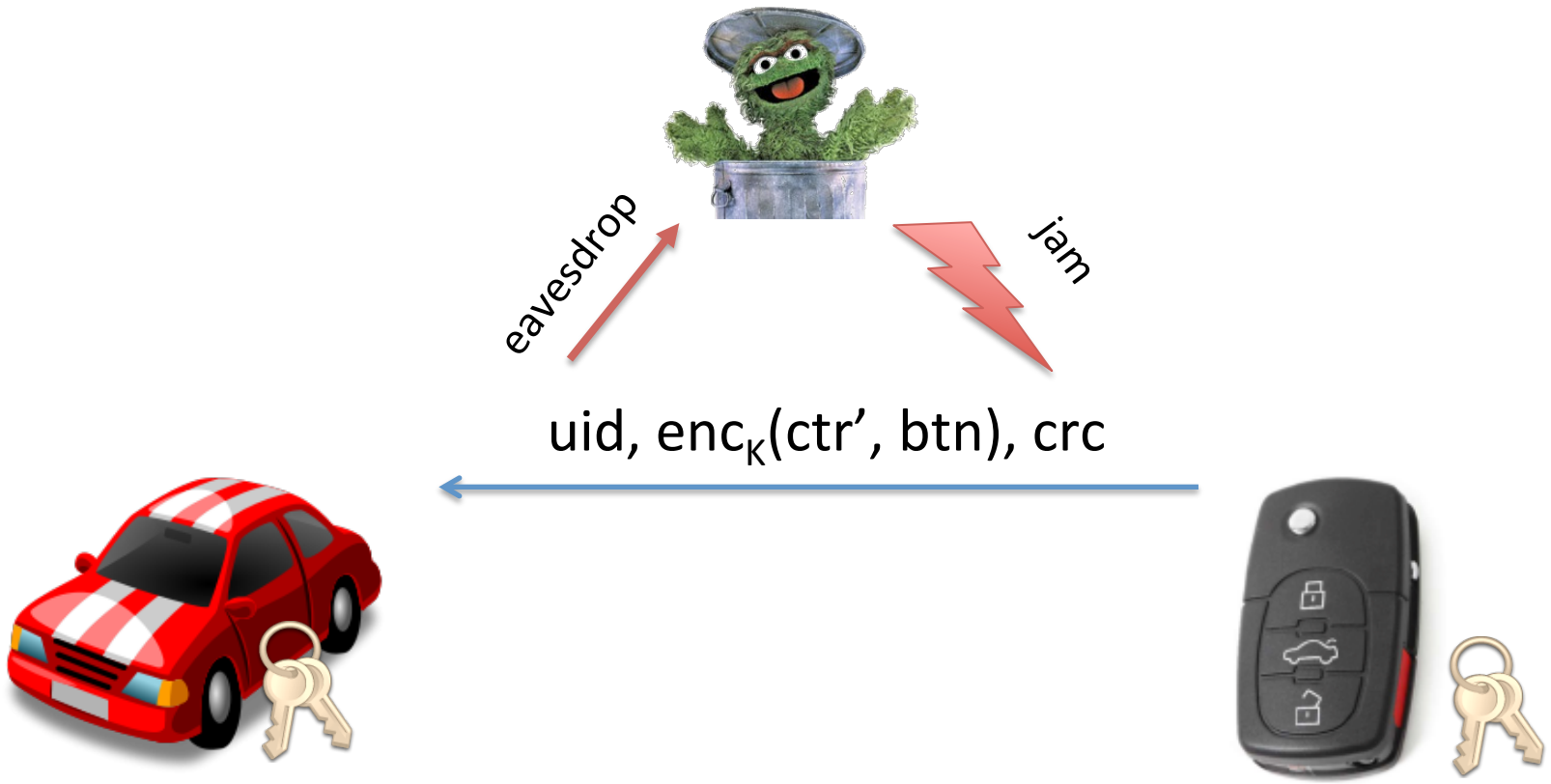
Derartige Fahrzeuge lassen sich starten, ohne dass ein Zündschlüssel in ein Zündschloss eingeführt wird. Vielmehr ist es für das Starten des Fahrzeugs ausreichend, dass sich der zugehörige Fahrzeugschlüssel oder die zugehörige Chipkarte im Fahrzeug befindet. Zudem lassen sich die verschlossenen Fahrzeuge öffnen, wenn sich der Schlüssel im unmittelbaren Umfeld des Fahrzeugs befindet.

Die hier agierende Tätergruppe, zu der auch der Angeklagte zählen soll, habe sogenannte „Mobi-Finder“ als Repeater verwendet, mit welchen das Funksignal der in der Wohnung der Geschädigten befindlichen Fahrzeugschlüssel aufgegriffen und weiter-

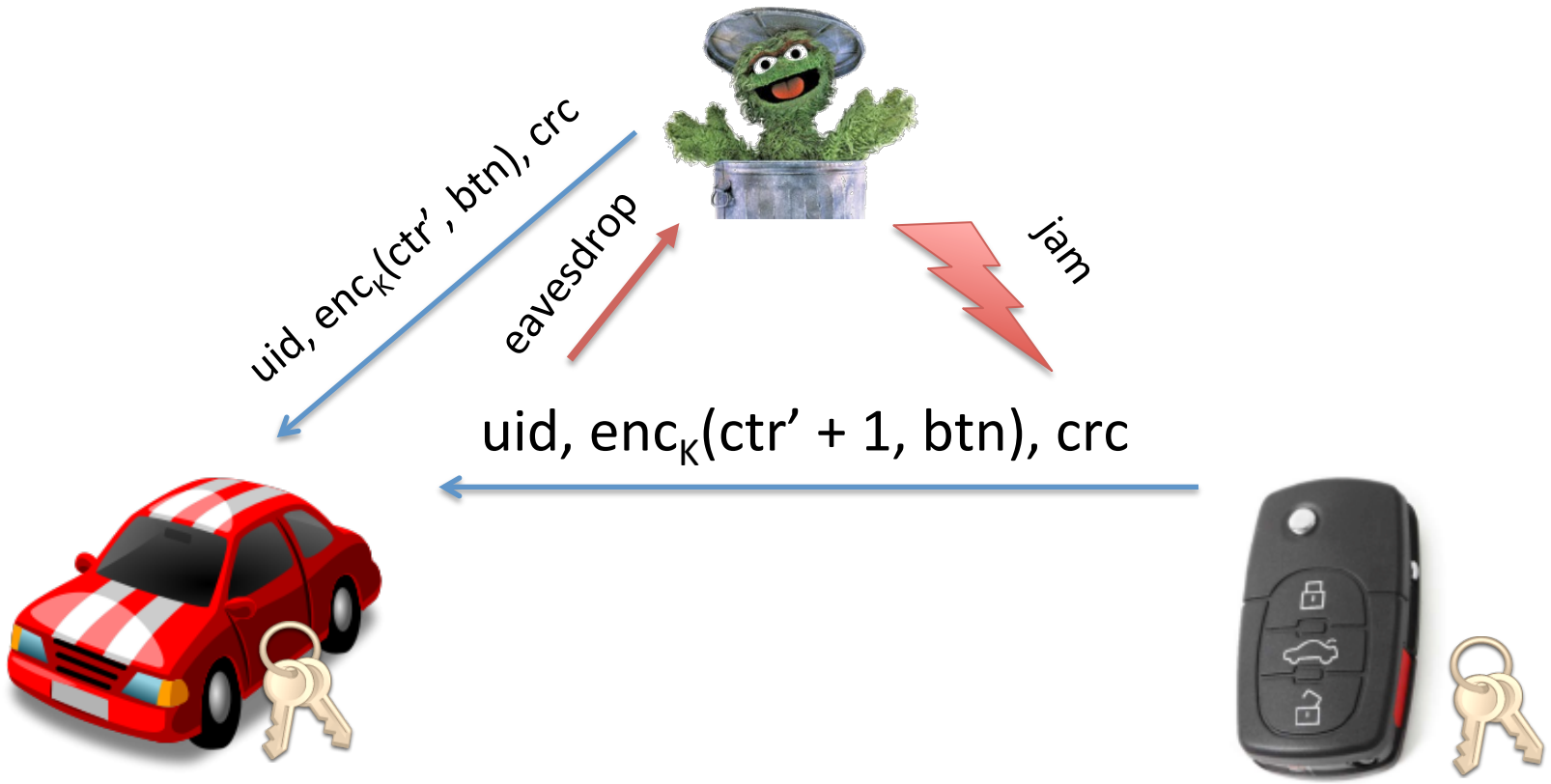
Previous attacks on RKE

- 2007: Cryptanalysis of KeeLoq garage door openers (2^{16} plaintext/ciphertext pairs) by Biham et al.
- 2008: Side-channel attack on KeeLoq key diversification (Eisenbarth et al.)
- 2010: Relay attacks on passive keyless entry systems (Francillon et al.)
- **2015: "RollJam" by Spencerwhyte / Kamkar**
  (had been proposed before)

“Intelligent jamming”



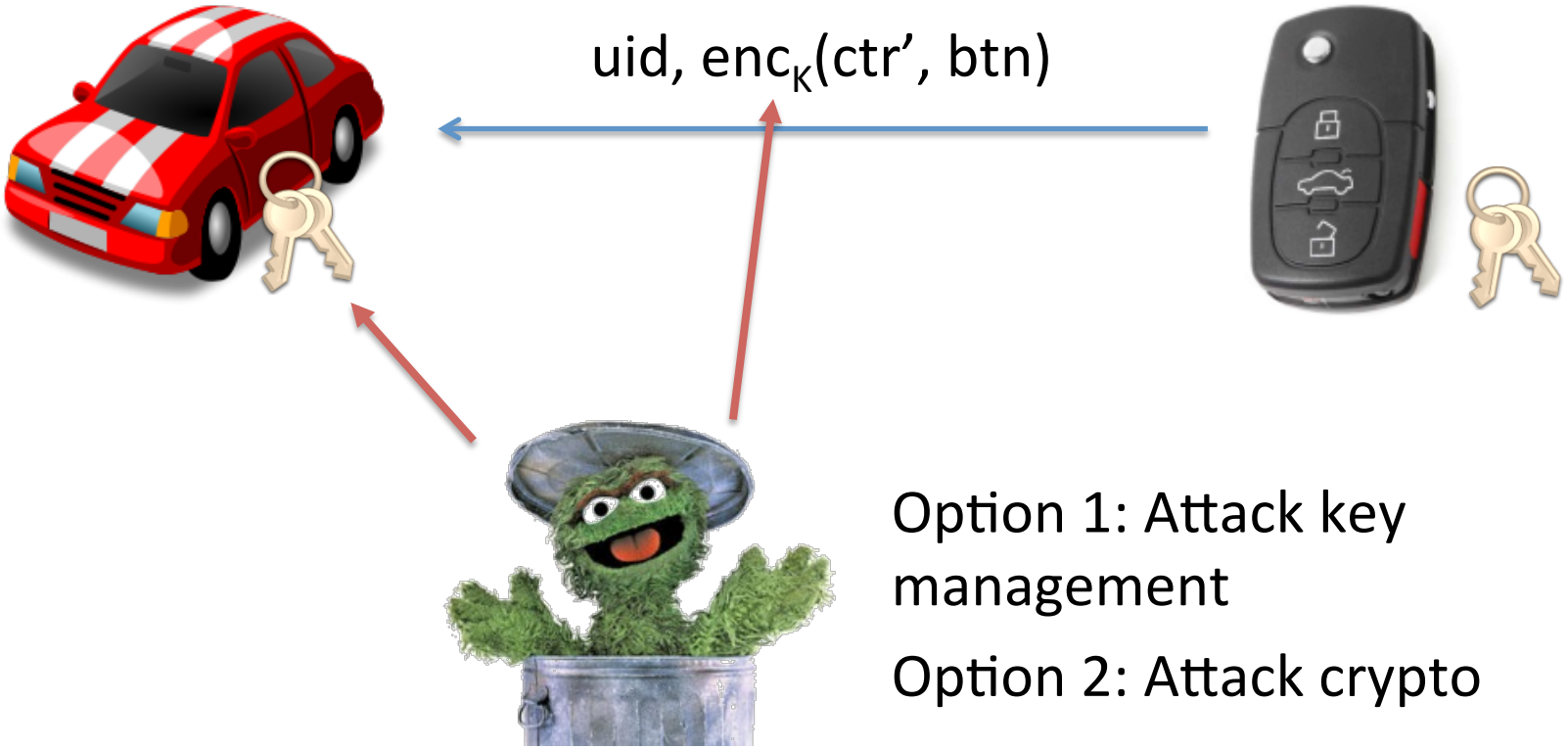
“Intelligent jamming”



Attacker now has another valid rolling code (ctr’ + 1)
However, cannot change btn!

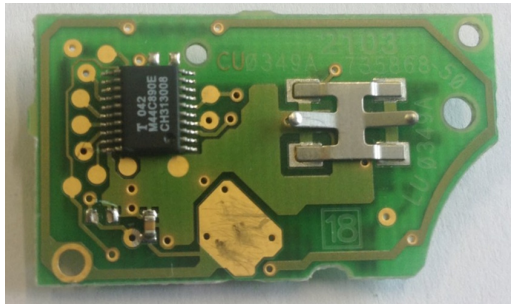
Question:
State of RKE security in 2016
(or: have we learnt from KeeLoq?)

Cryptographic attack surface

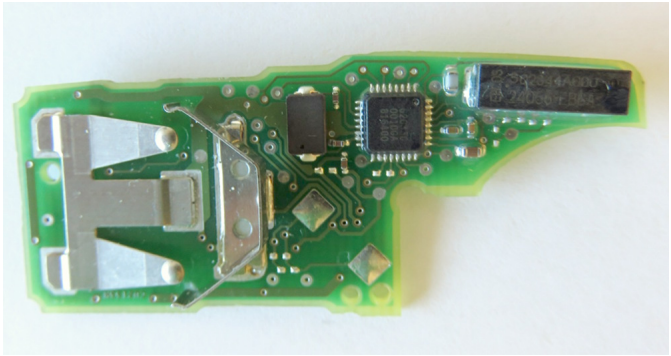


Option 1: Attack key management

Option 2: Attack crypto



The VW Group System

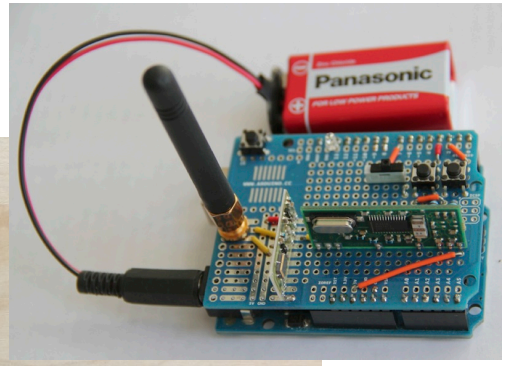


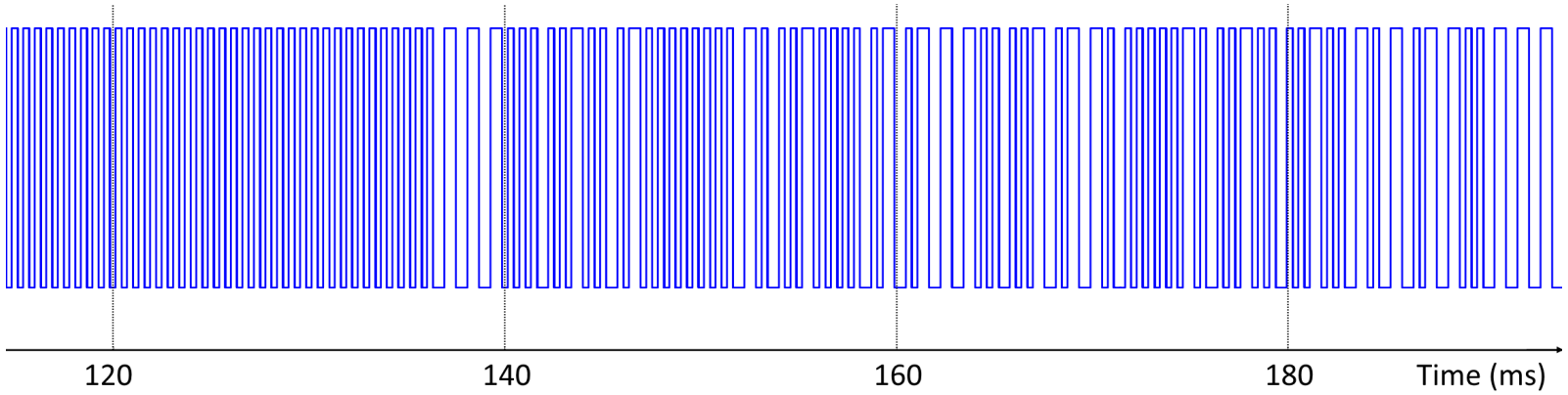
VW Group RKE

- > 10% worldwide market share
- Immobilizer (Megamos) and RKE separate for most vehicles
- Proprietary RKE system, mostly 434.4 MHz
- We analyzed vehicles between ~2000 and today
- Four main schemes (VW-1 … VW-4) studied

VW Group RKE: signals

Step 1: Eavesdropping & decoding

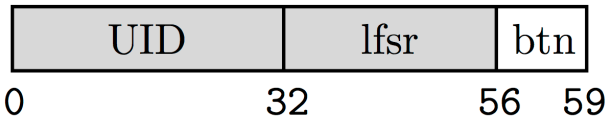




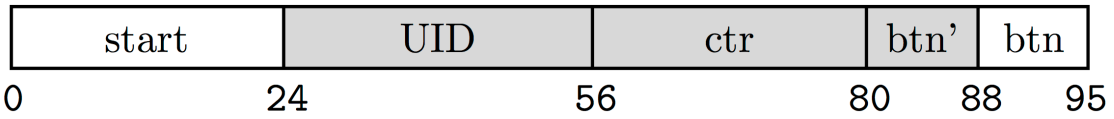
VW Group RKE: signals

Step 1: Eavesdropping & decoding

- VW-1:



- VW-2 … 4:



Analyzing ECUs

Step 2: Obtain ECUs for analysis (eBay) ...

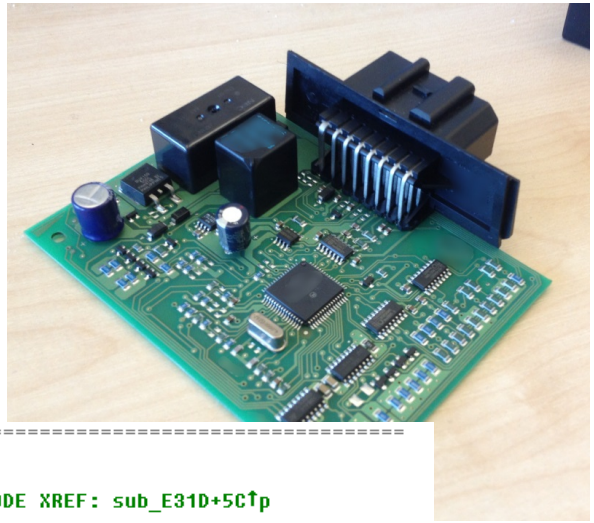
Staropramen

8x660ml e


1869
Staropramen
8x660ml e

Reverse engineering

Step 3: Reverse-engineering ECUs



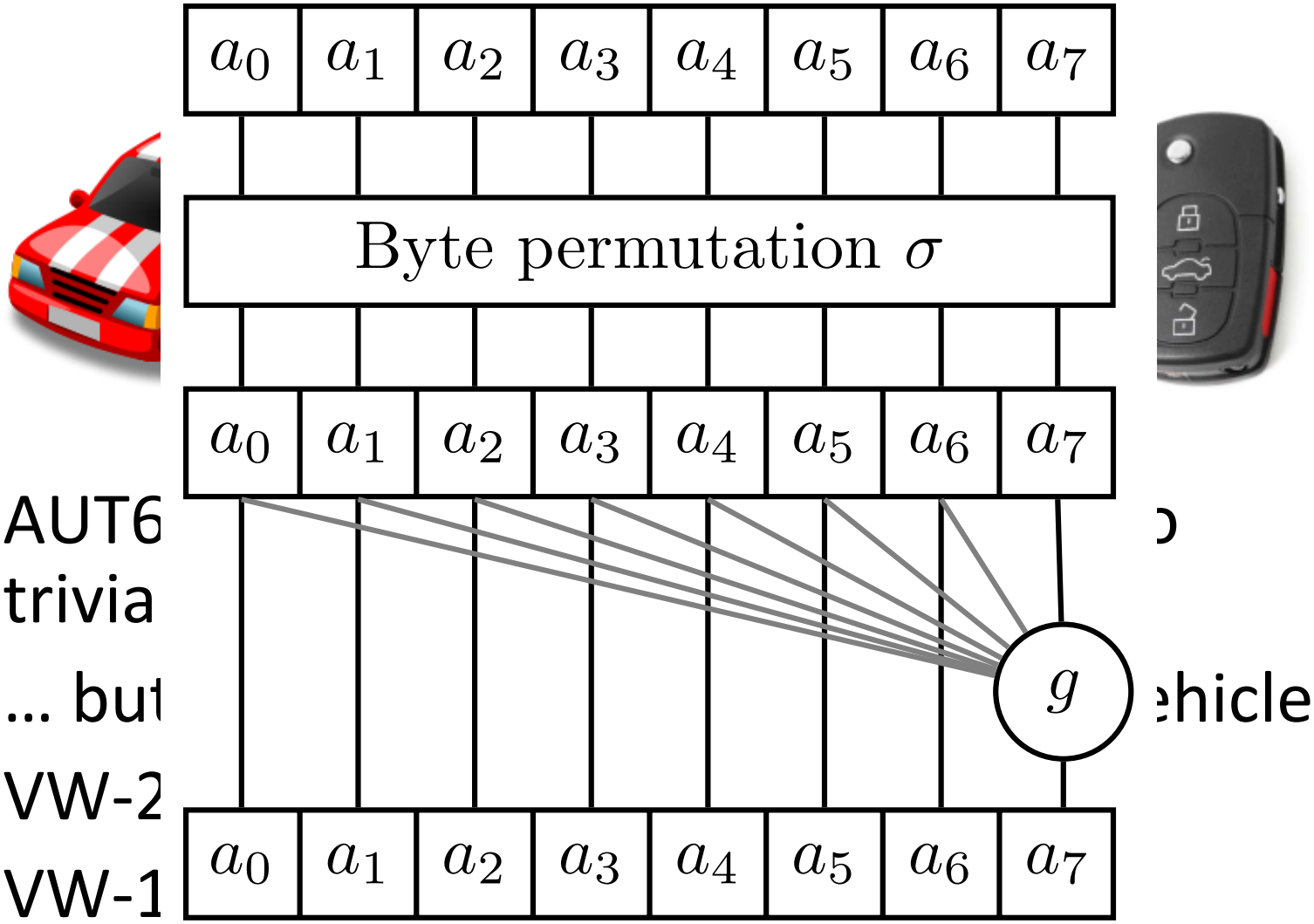
```
; =============== S U B R O U T I N E =======================================

sub_F5C4:                               ; CODE XREF: sub_E31D+5C↑p
                pshd
                pshx
                leas    -$C,sp
                anda    #$3F ; '?'
                clrx
                addd    #$8000
                bcc     loc_F5D2
                inx

loc_F5D2:                               ; CODE XREF: sub_F5C4+B↑j
                std     4,sp
                ldd     $14,sp
                ldx     $12,sp
                subd    $E,sp
                sbex    $C,sp
```

Example: VW-3

$AUT64_{K_3}(uid, ctr', btn'), btn$

- AUT64 is a proprietary block cipher, no trivial attacks known
- … but key K_3 is the same in **all** VW-3 vehicles
- VW-2: Same cipher, different key
- VW-1: Weak crypto (LFSR)

Example: VW-2



- AUT6 … trivia
- … but … ehicles
- VW-2
- VW-1

Example: VW-4

$XTEA_{K_4}(uid, ctr', btn'), btn$

- Used from ~ 2010 onwards
- Secure standard cipher: XTEA
- … but again one worldwide key K_4
- Adversary can clone remote by eavesdropping a single rolling code

Affected vehicles

- **Audi**: A1, Q3, R8, S3, TT, other types of Audi cars (e.g. remote control 4D0 837 231)
- **VW**: Amarok, (New) Beetle, Bora, Caddy, Crafter, e-Up, Eos, Fox, Golf 4, Golf 5, Golf 6, Golf Plus, Jetta, 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, Yeti
- **In summary:** probably most VW group vehicles between 2000 and today not using Golf 7 (MQB) platform

VW RKE demo

Intermezzo

- Cryptographic algorithms improving over time, but: Secure crypto ≠ secure system
- Reverse engineering ECU firmware yields a few worldwide keys
- Attack highly practical and scalable
- MQB allegedly protected
- Seems worse compared to KeeLoq (’08), actually quite similar though

The Hitag2 System

Previous work on Hitag2

- At Usenix Security ’12, Verdult et al. presented a secret key recovery attack against Hitag2 **immobilizer** requiring:
  - Immobilizer transponder **uid**
  - **136** authentication attempts from the car
  - 5 minutes computation
- Note: This attack is not car-only due to the first requirement

Hitag2 RKE: Our contribution

- Step 1: Black-box reverse engineering of RKE protocol
  - Known cipher and inputs
  - Trial-and-error, guessing probable implementations
- Step 2: 136 traces is not practical in a RKE context; need for improved attack

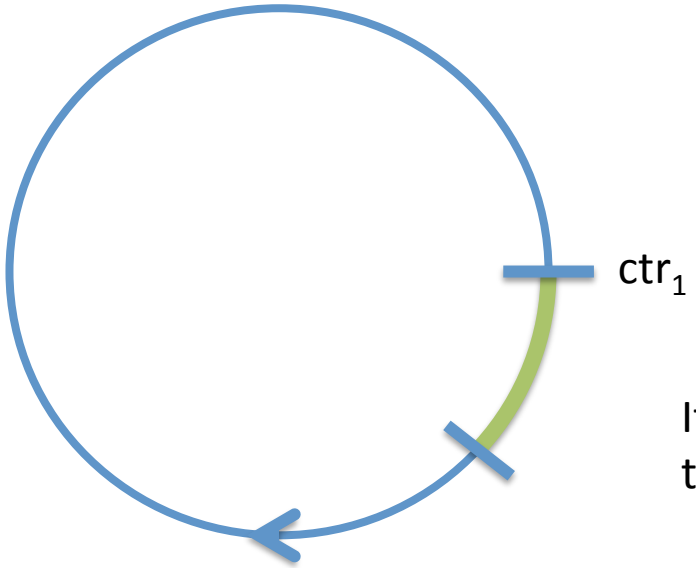
RKE protocol (simplified)

MAC_k is 32 bits of keystream

uid, btn, ctr, MAC_k, crc

Diversified keys

id_1	k_1	ctr_1
id_2	k_2	ctr_2
id_3	k_3	ctr_3



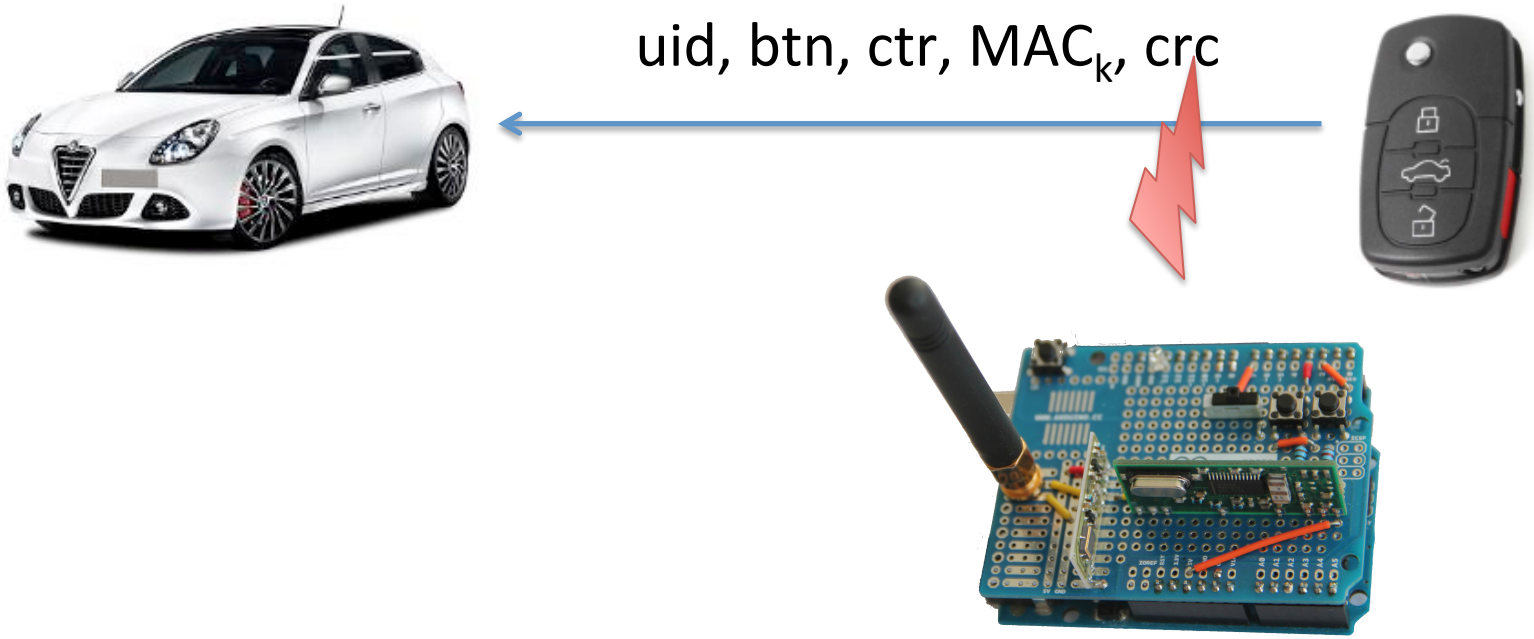
If ($ctr_1 < ctr'_1 < ctr_1 + \Delta$)
then $ctr_1 := ctr'_1$; open

A few observations

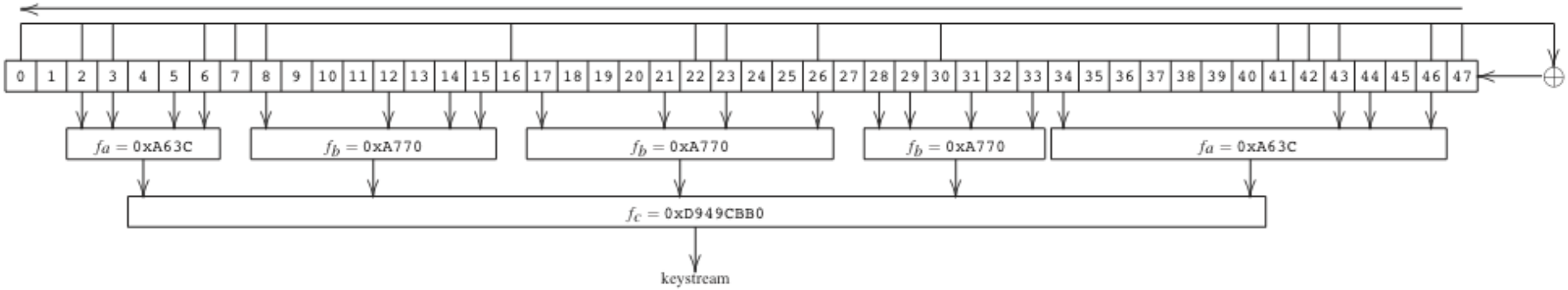
- Put uid, btn, ctr, key into Hitag2, MAC is 32 bit of keystream
- Only a few bit difference in input for subsequent protocol runs (ctr and btn change)
- Hybrid chip (Immo + RKE) uses a different secret key but the **same uid** (can be eavesdropped from 100 m)
- Hitag2 systems have diversified keys

Our novel attack requires:

- ≈ 4 to 8 traces (key presses)
- $40 Arduino board can collect them
- Speeding up trace collection:
  Device also implements reactive jamming:



Hitag2 cipher



48 bit internal state (LFSR stream a_0a_1…)

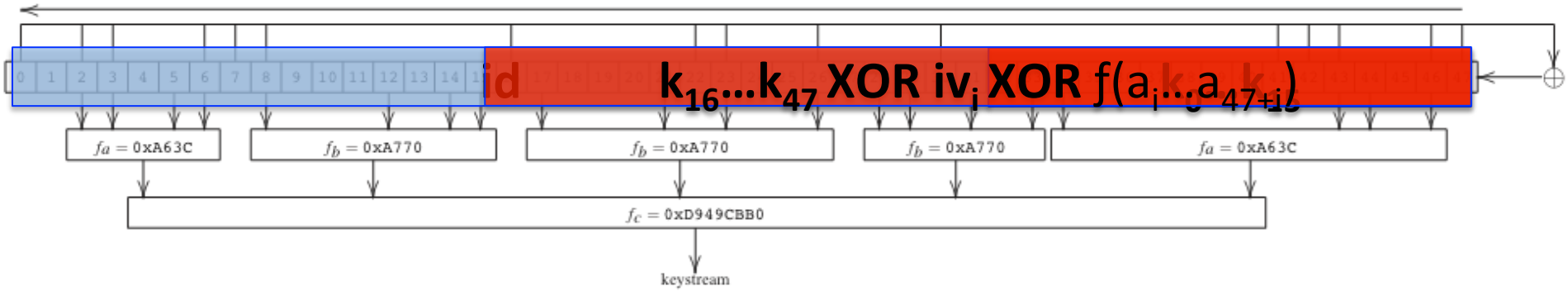
$a_0 \ldots a_{31} = id_0 \ldots id_{31}$

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

$a_{48+i} = k_{16+i} \oplus \{data\}_i \oplus f(a_i \ldots a_{47+i})$

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

Hitag2 cipher



48 bit internal state (LFSR stream a_0a_1…)

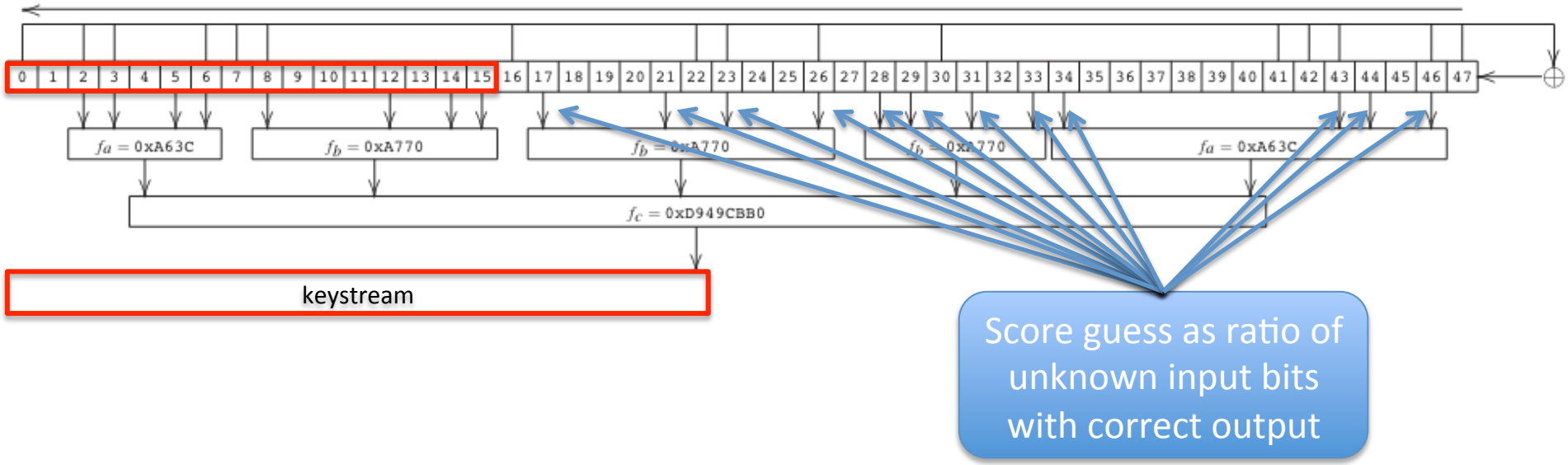
$a_0…a_{31} = id_0…id_{31}$

$a_{32}…a_{47} = k_0…k_{15}$

$a_{48+i} = k_{16+i} \oplus iv_i \oplus f(a_i…a_{47+i})$

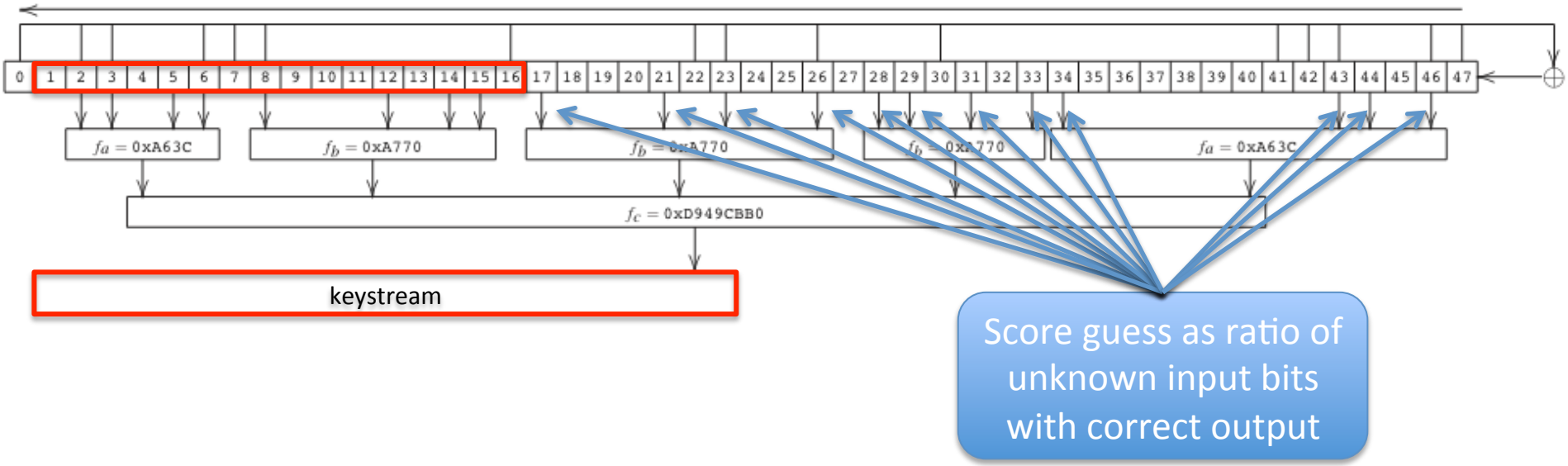
Initialized LFSR = $a_{32}…a_{79}$

A fast correlation attack on Hitag2 (simplified)

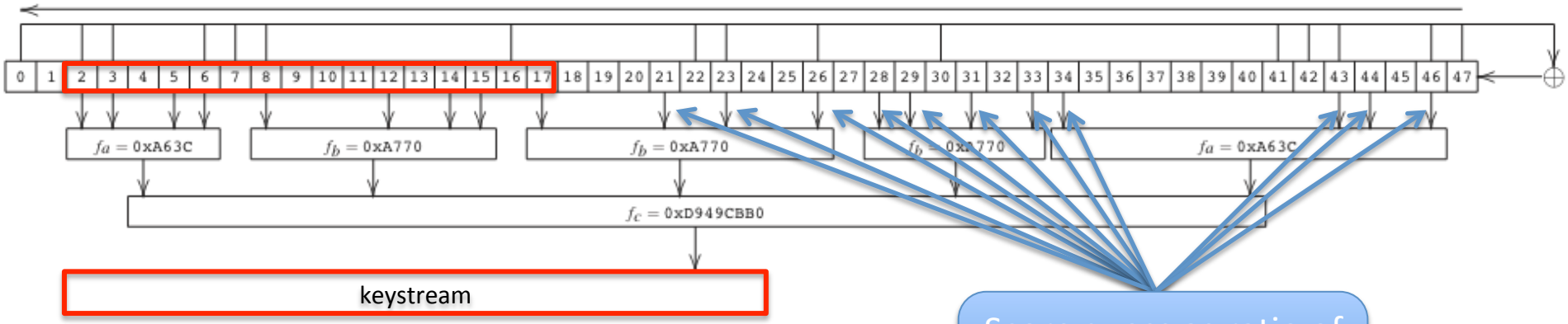


- Guess a 16-bit window value

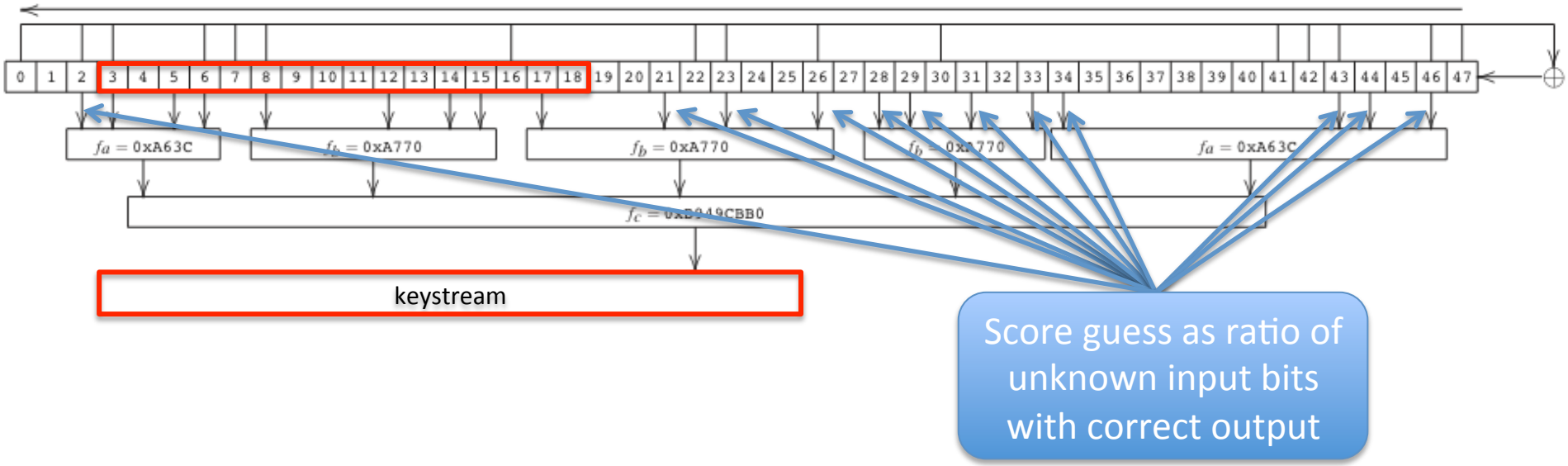
A fast correlation attack on Hitag2 (simplified)



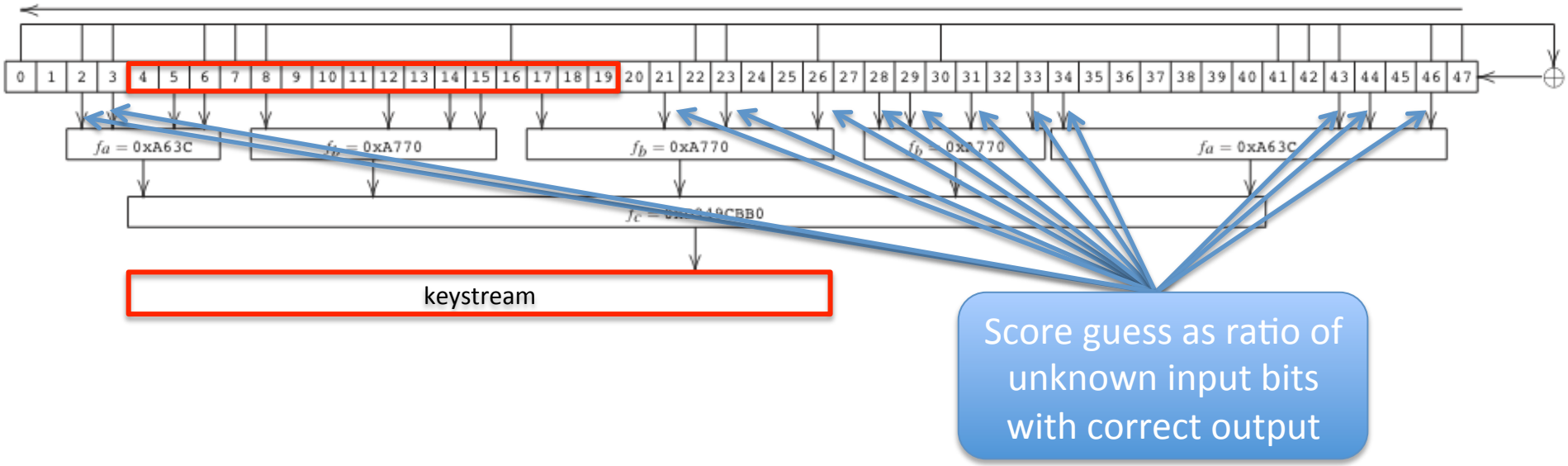
A fast correlation attack on Hitag2 (simplified)



A fast correlation attack on Hitag2 (simplified)



A fast correlation attack on Hitag2 (simplified)



- Discard overall low scoring guesses
- Increase window size by one
- Repeat
- Takes ~**1 minute** on a laptop to recover the key

Practical limitations

- Only the 10 LSBs of the counter are sent over the air, but all 28 bits are used
  - we need to guess 18 MSBs -> surprisingly easy as they start from **zero**
- Attack works with 4 traces for Immo, as it uses a random challenge. RKE traces give out less information so we need more, usually 8.

UID	btn	ctr	challenge	MAC	crc
5ad40e29	08	0294	0000e948	27ee2032	1e
5ad40e29	08	0295	0000e958	2dee2f1e	be
5ad40e29	08	02a9	0000ea98	220d918e	45
5ad40e29	08	02ab	0000eab8	2a0f91e8	fc
5ad40e29	08	0338	0000f388	08f405c9	07
5ad40e29	08	033a	0000f3a8	08f48d8a	20

Hitag2 RKE attack demo

Hitag2 RKE vehicles

Manufacturer	Model	Year
Alfa Romeo	Giulietta	2010
~~Chevrolet~~	~~Cruze Hatchback~~	~~2012~~
Citroen	Nemo	2009
Dacia	Logan II	2012
Fiat	Punto	2016
Ford	Ka	2009, 2016
Lancia	Delta	2009
Mitsubishi	Colt	2004
Nissan	Micra	2006
Opel	Vectra	2008
Opel	Combo	2016
Peugeot	207	2010
Peugeot	Boxer	2016
Renault	Clio	2011
Renault	Master	2011
Opel	Astra H	2008
Opel	Corsa D	2009
Fiat	Grande Punto	2009

RKE system in some cars…

State:

id_1	k_1	ct
id_2	k_2	ctr_2
id_3	k_3	ctr_3

ctr_1

If (ctr_1- Δ < ctr'_1 < ctr_1 + Δ)
then ctr_1 := ctr'_1 ; open

Have we learnt from KeeLoq?

Not really

Countermeasures:
What to do?


KAOS


ALARM
ESSO

Countermeasures

Table 4-1. RKE Message Payload

Byte No.	Data Type	Description
1-4	UID(32b)	32-bit unique device ID
5	CMD(8b)	8-bit command
6-9	CNTR(32b)	32-bit counter value
10-17	MAC(56b)	Option A: $Enc_{AES\text{-}128}((UID, CMD, CNTR, 0_{56}), 56)$ Option B: $Enc_{AES\text{-}128}((UID, CMD, CNTR, UID_{24}), 56)$
18	CRC-8	Payload data checksum

http://www.atmel.com/Images/Atmel-9224-Key-Fob-Design-Based-on-Atmel-ATA5795_Application-Note.pdf

- For manufacturers:
  - Use secure key distribution and good crypto
  - E.g. exchange keys via LF (immo) once and use AES for RKE

Responsible disclosure

- We contacted VW Group in Dec 2015 and NXP Semiconductors in Jan 2016
- In general: good cooperation/ communication
- VW Group claims that MQB has diversified keys
- NXP has AES-based products

Conclusio

- Poor crypto is bad …
- Poor key management i
- Finding widespread exa
  was rather surprising in
- This research may expla
  mysterious theft cases v
  forced entry

Your car is not a safe box

Thanks for your attention!

Questions?

UNIVERSITY OF BIRMINGHAM

KASPER OSWALD

Innovative Security Engineering