Lock It and Still Lose It - On the (In)Security of Automotive Remote Keyless Entry Systems

Flavio D. Garcia[1], David Oswald[1],
Timo Kasper[2] and Pierre Pavlidès[1]

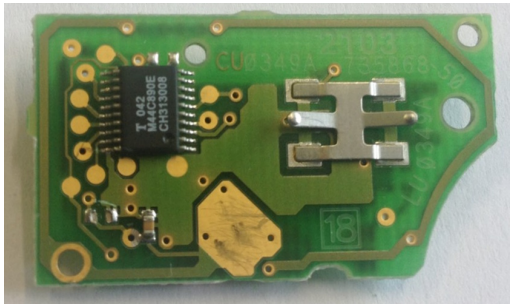
1. University of Birmingham, UK
2. Kasper & Oswald GmbH, Germany

Immobilizer (Immo)

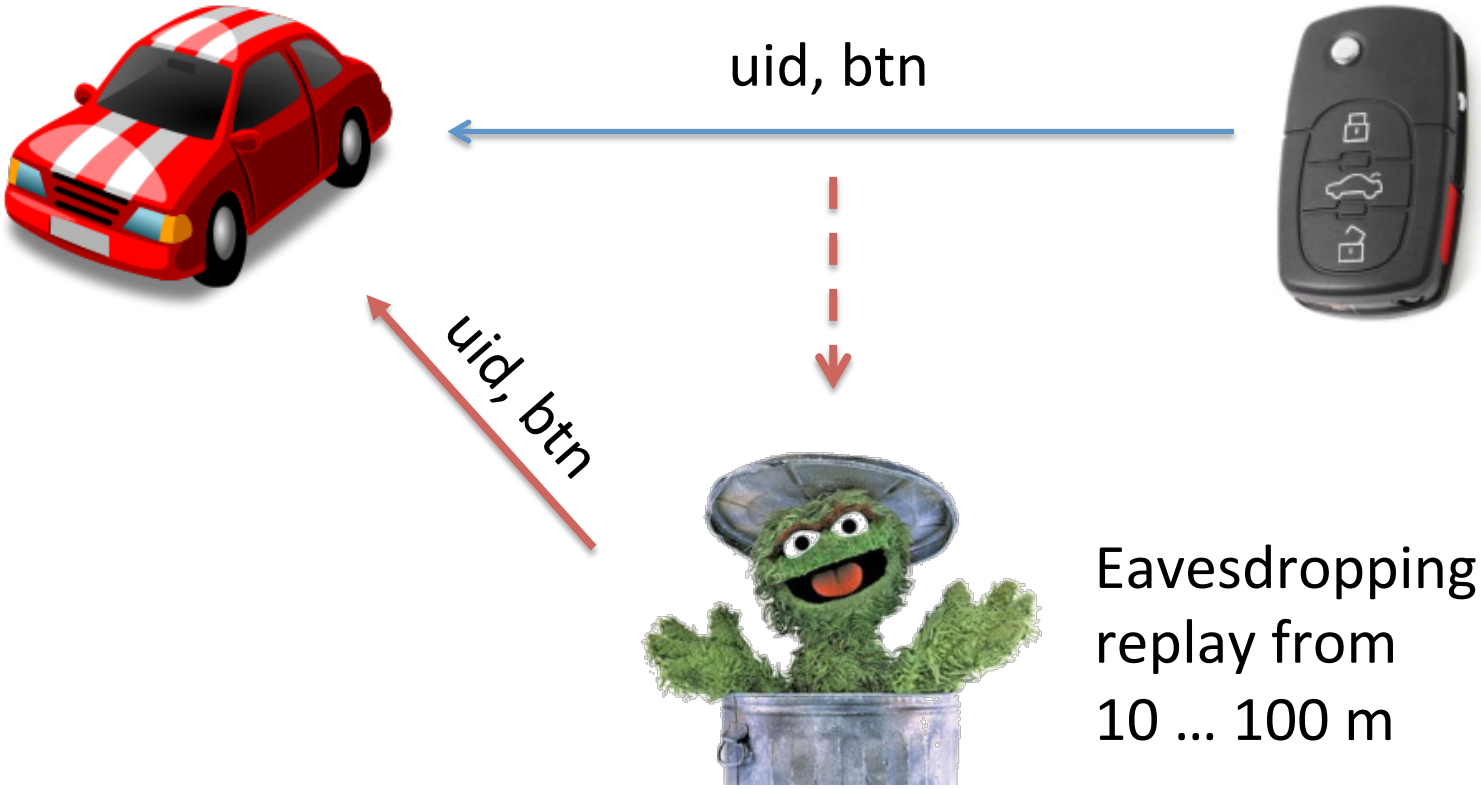
- Passive RFID at 125 kHz
- Many broken systems (DST40, Hitag2, Megamos)

Remote Keyless Entry (RKE)

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



History of RKE: Fix Codes



Eavesdropping and replay from 10 … 100 m

History of RKE: Rolling Codes

$uid, enc_K(ctr', btn)$

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

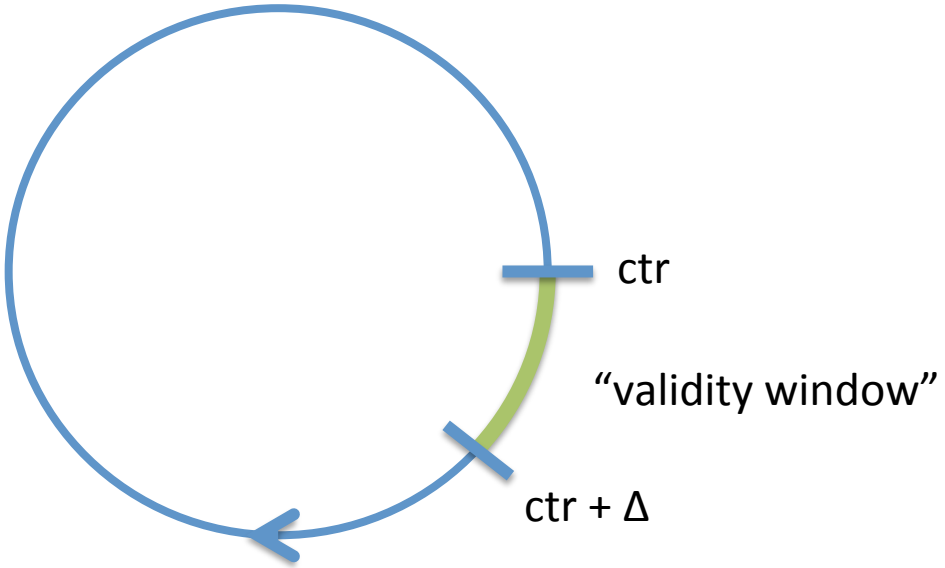
$uid, enc_K(ctr' + 2, btn)$

Decrypt ctr'

if (ctr < ctr' < ctr + Δ)

ctr := ctr'

open / close



History of RKE: Rolling Codes

uid, $enc_K(ctr', btn)$

ctr' incremented on each button press, replay fails

History of RKE: Rolling Codes

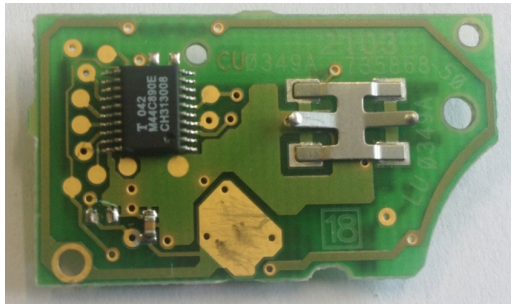
uid, $enc_K(ctr', btn)$

Option 1: Attack key management

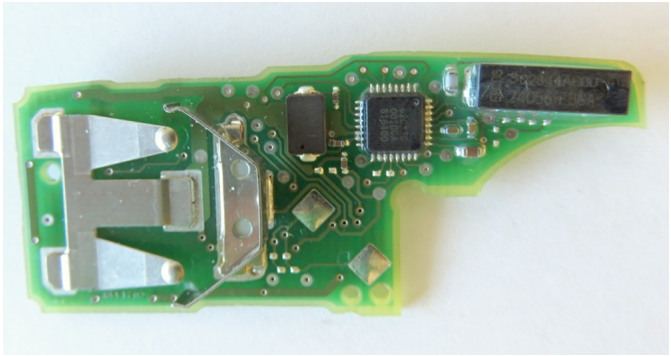
Option 2: Attack crypto

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.)
- 2014: Cesare: attack on 2000 – 05 vehicle
- 2015: "RollJam" by Spencerwhyte / Kamkar
  (had been proposed before, does not apply to most modern vehicles since button is authenticated)



Part 1: The VW Group System

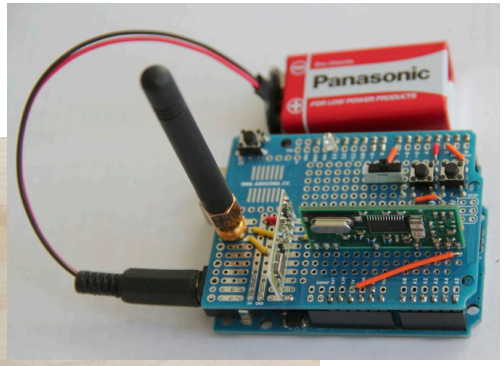


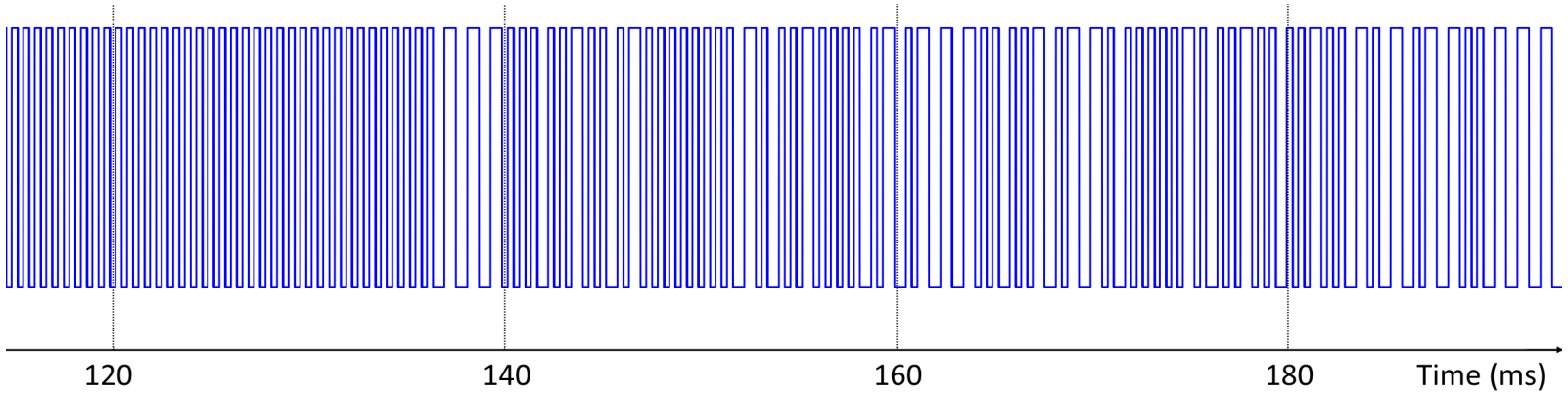
VW Group RKE

- > 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: Analysis

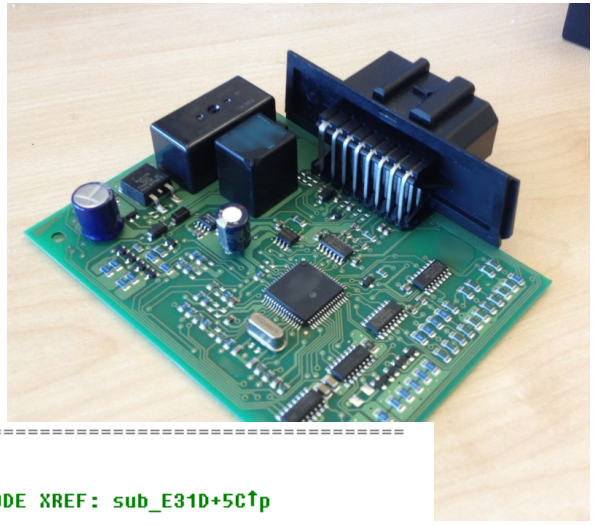
Step 1: Eavesdropping & decoding





VW Group RKE: Analysis

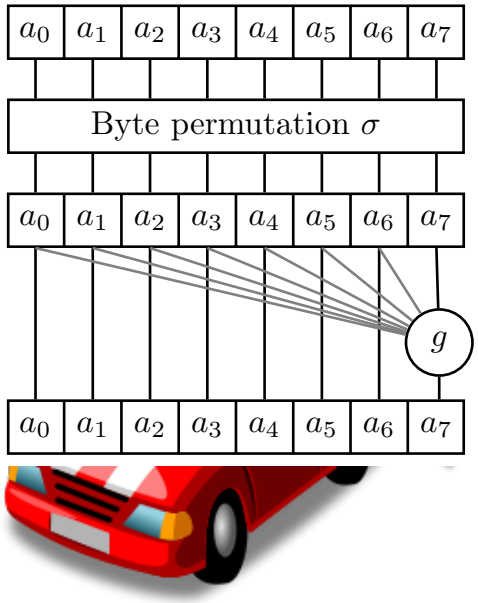
Step 2: Reverse-engineering ECUs



```
; =============== 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
```



xample: 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-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

VW RKE Demo

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

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
- New VW group system (MQB / Golf 7) allegedly uses diversified keys + good crypto

Part 2: The Hitag2 System

Hitag2 Usage in RKE

Our previous work on Hitag2

- At Usenix Security'12 we presented a secret key recovery attack against Hitag2 **immobilizer** requiring:
  - Immobilizer transponder **uid**
  - **136** authentication attempts from the car
  - 5 minutes computation
- This attack was not considered car-only due to the first requirement.

In the RKE context

- Hybrid chip (Immo+RKE) uses a different secret key but the **same uid**
  - This can be eavesdropped from 100 m/300 ft
- **136** traces is not practical in a RKE context, so we needed to improve the attack

The cipher was known so we did a black-box reverse engineering of the protocol

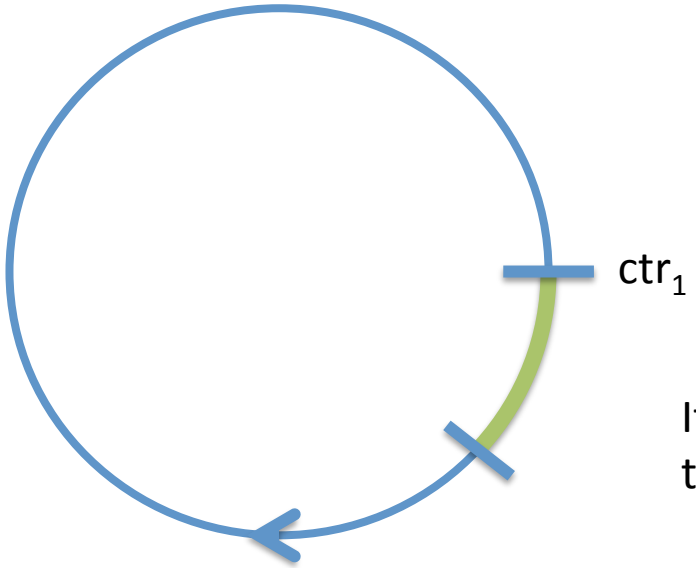
RKE Protocol (simplified)

MAC_k is just 32 bits of keystream

uid, btn, ctr, MAC_k, crc

State:

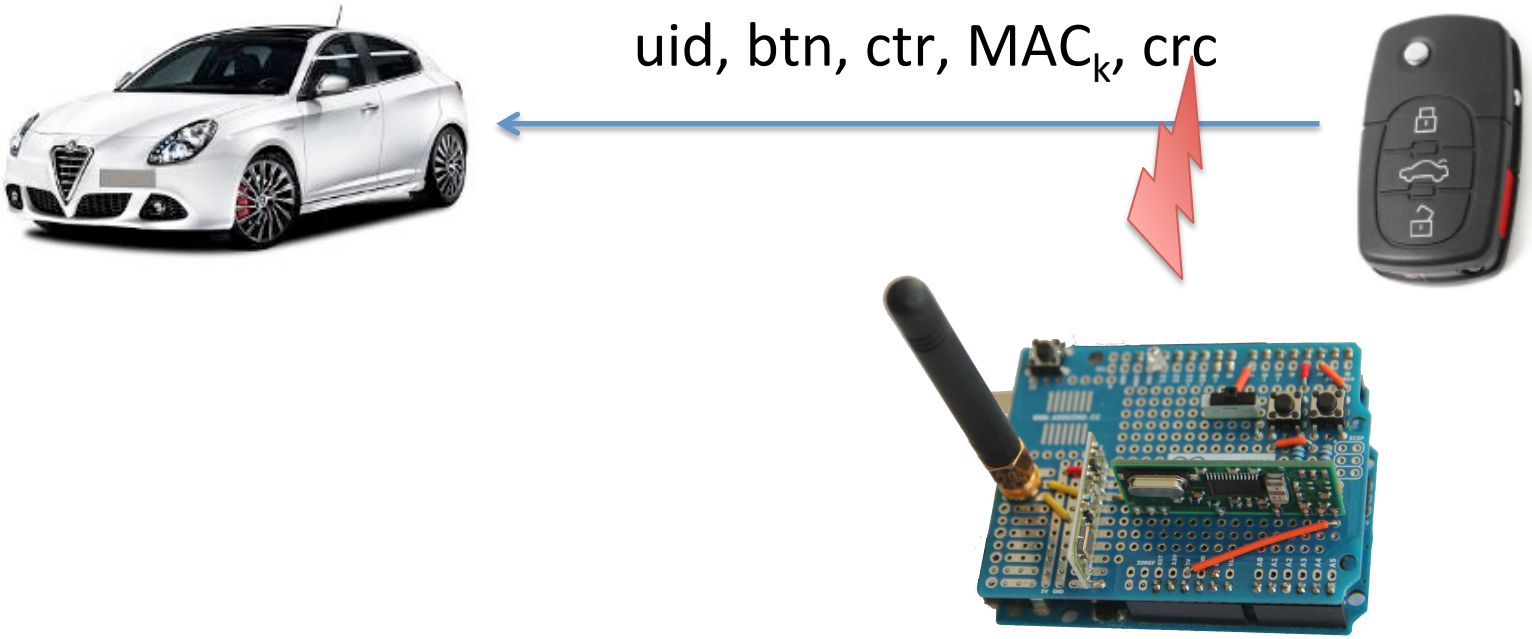
id_1	k_1	ctr_1
id_2	k_2	ctr_2
id_3	k_3	ctr_3



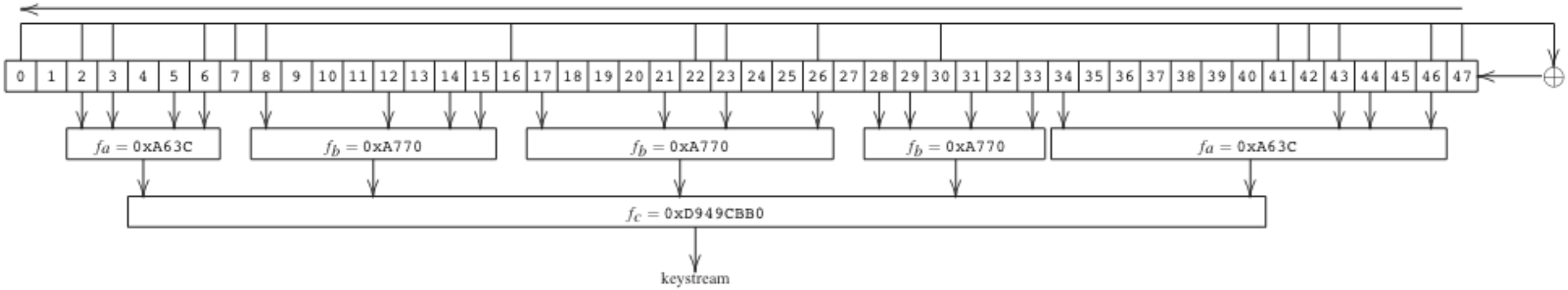
If ($ctr_1 < ctr'_1 < ctr_1 + \Delta$)
then $ctr_1 := ctr'_1$; open

Our RKE attack requires

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



Hitag2 Cipher



48 bit internal state (LFSR stream a_0a_1…)

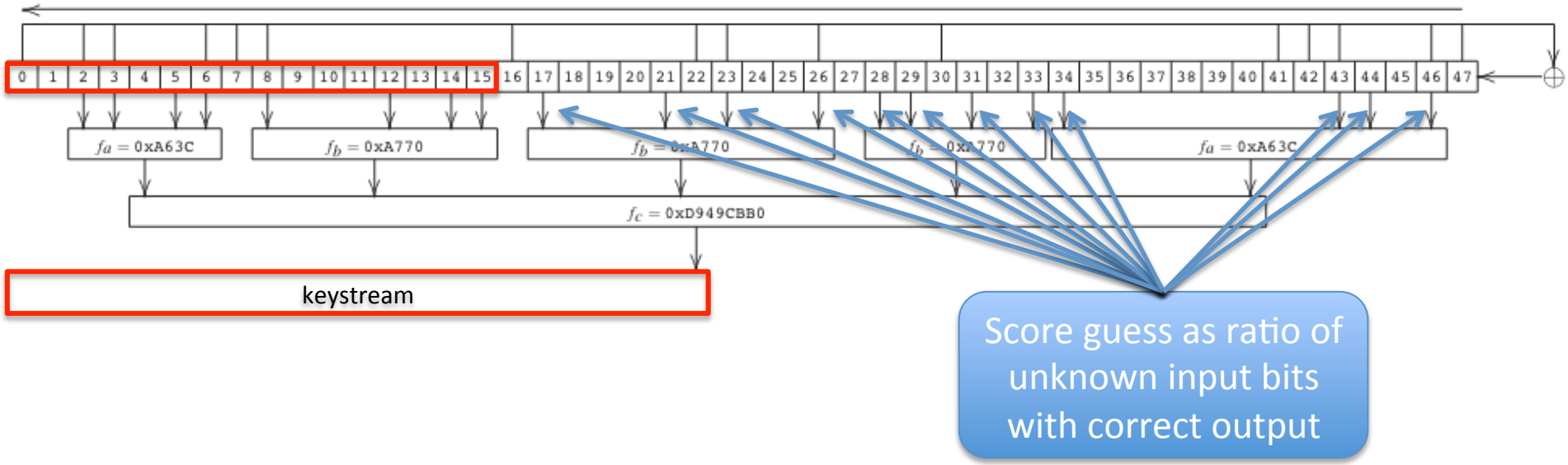
$a_0 \ldots a_{31} = id_0 \ldots id_{31}$

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

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

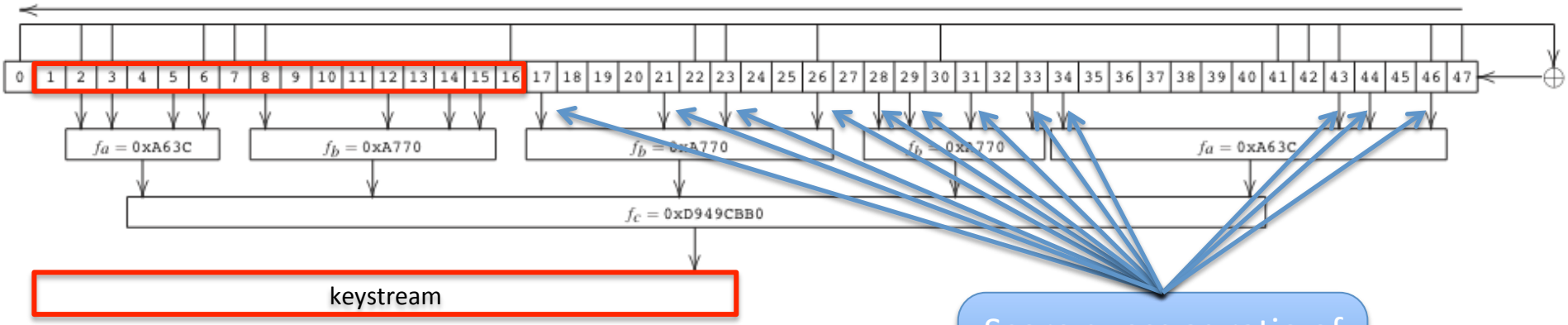
Initialized LFSR = $a_{32} \ldots a_{79}$

A fast correlation attack on Hitag2 (simplified)



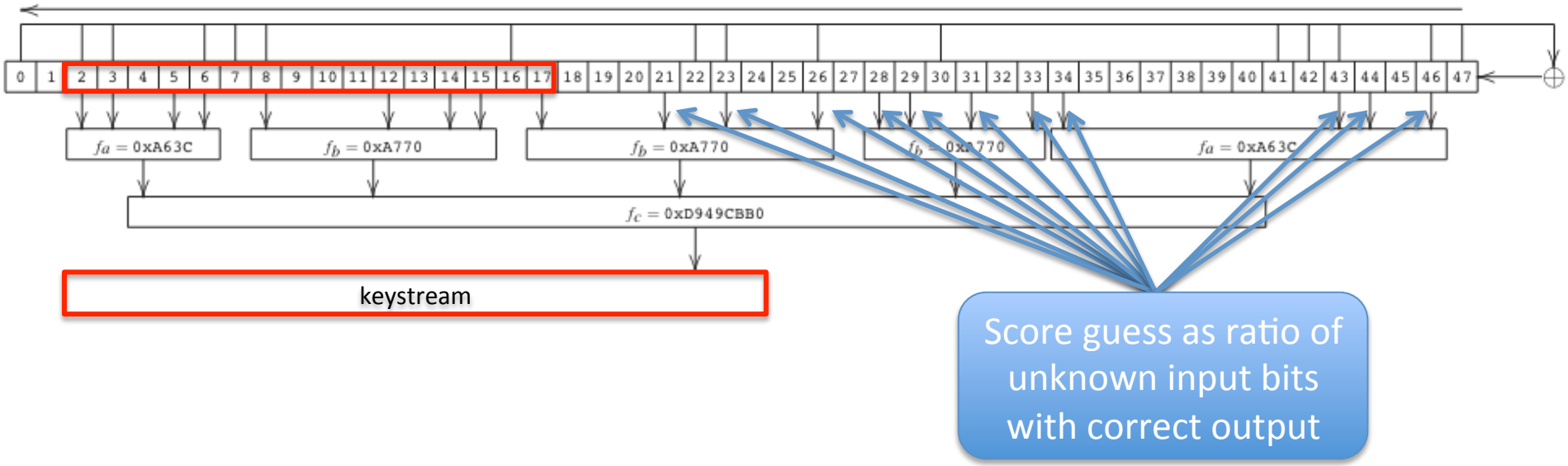
- Guess a 16-bit window value

A fast correlation attack on Hitag2 (simplified)

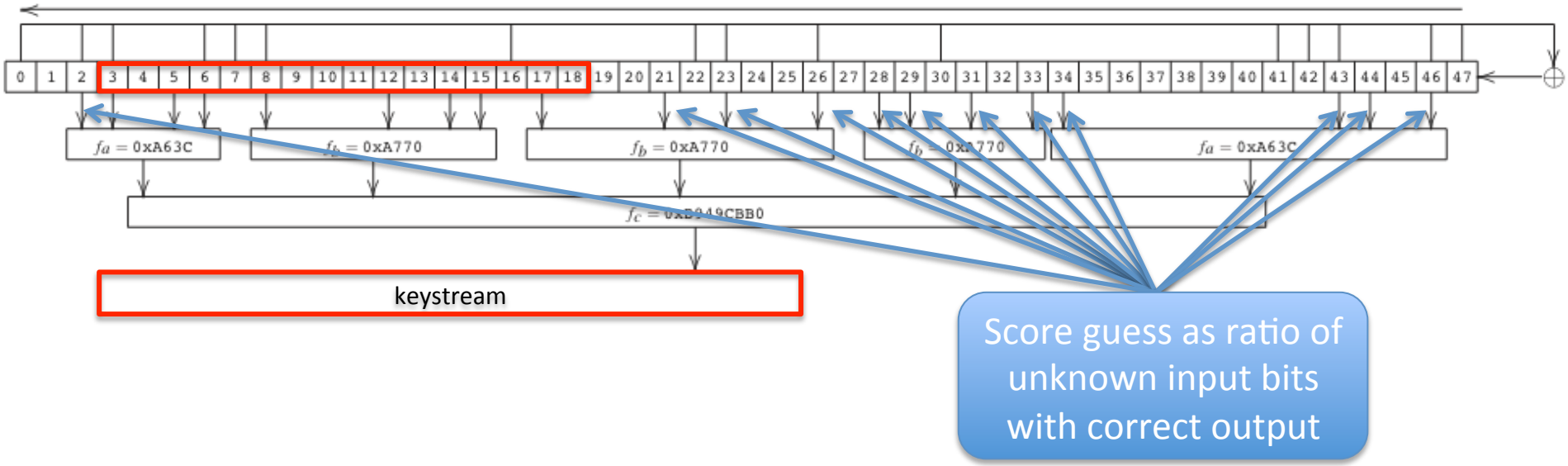


Score guess as ratio of unknown input bits with correct output

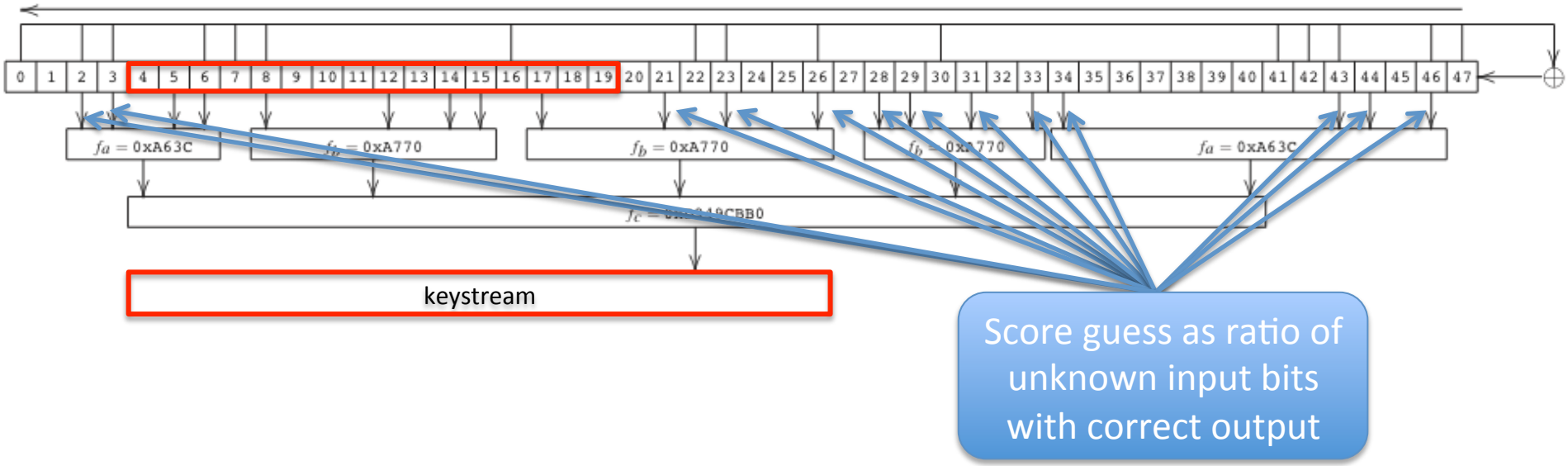
A fast correlation attack on Hitag2 (simplified)



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

Vehicles we tested using Hitag2 RKE

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

Conclusions

- We informed VW Group of our findings in back in Dec 2015 and NXP Semiconductors in Jan 2016.
- Weaknesses in the Hitag2 cipher known for many years but still used in new (2016) vehicles
- Poor crypto is bad, but poor key management is worse
- This research may explain several mysterious theft cases without signs of forced entry