Messing around with Garage Doors

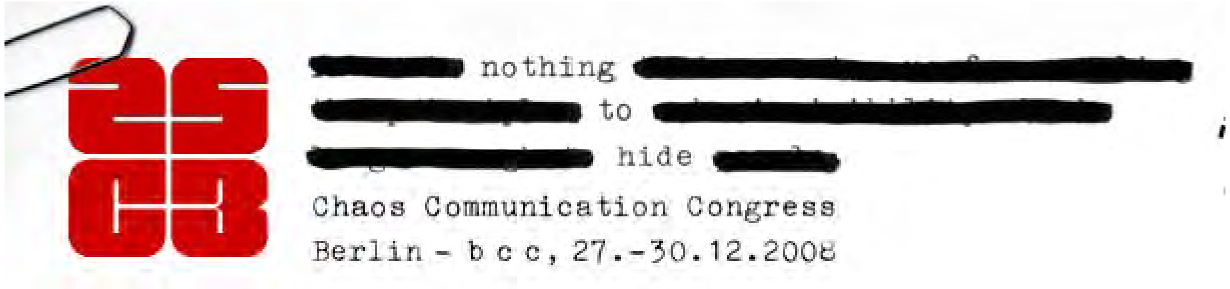
Breaking *KeeLoq* with Power Analysis

Thomas Eisenbarth & Timo Kasper

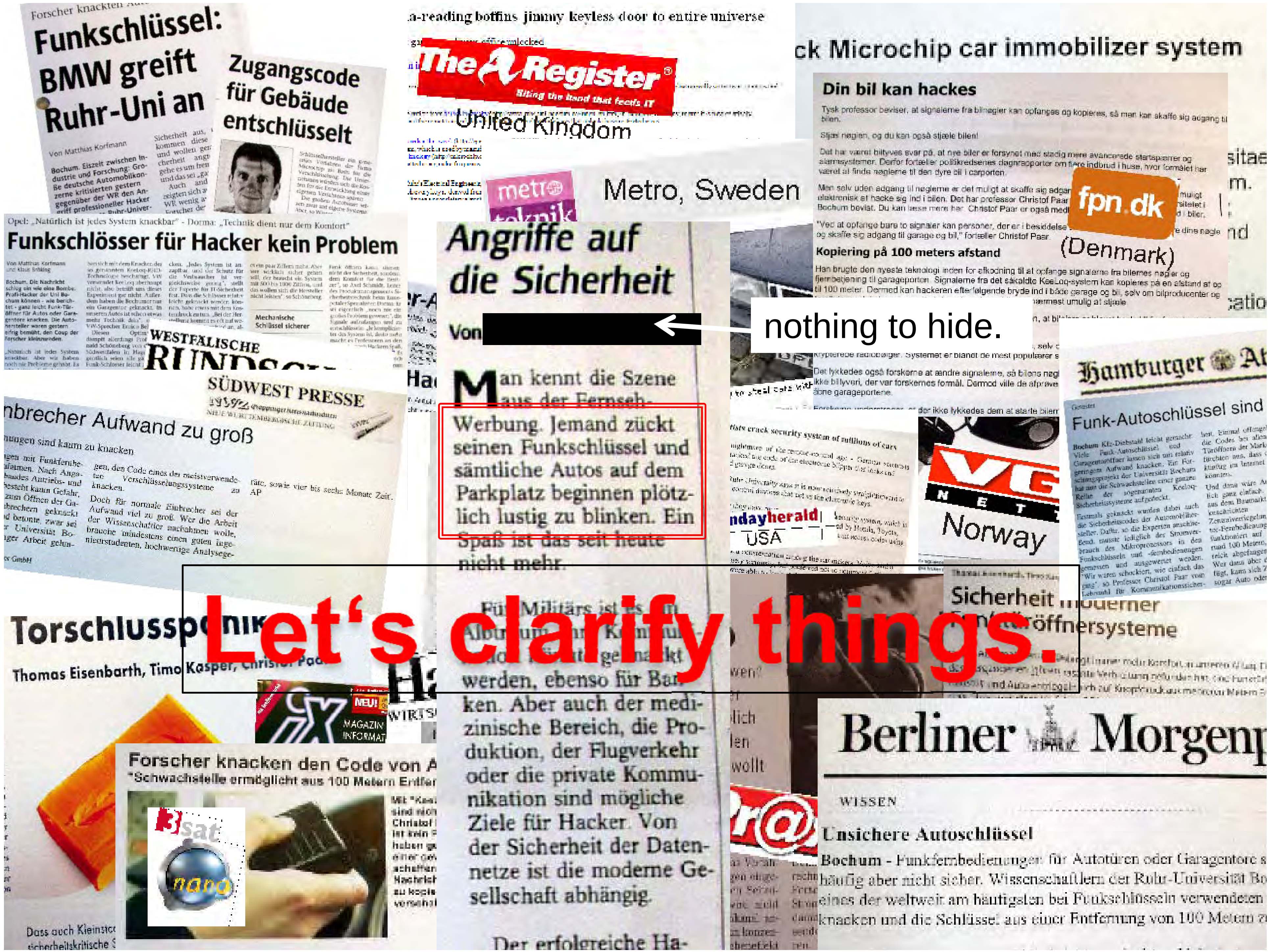
Embedded Security Group EMSEC (Prof. Paar)

Horst Görtz Institute for IT Security

Ruhr-University Bochum, Germany


[redacted] nothing [redacted]
[redacted] to [redacted]
[redacted] hide [redacted]
Chaos Communication Congress
Berlin - b c c, 27.-30.12.2008

Berlin, 27. December 2008



Forscher knackten Au

Funkschlüssel: BMW greift Ruhr-Uni an

Von Matthias Korfmann

Bochum. Eiszeit zwischen Industrie und Forschung: Große deutsche Automobilkonzerne kritisierten gestern gegenüber der WR den Angriff professioneller Hacker Ruhr-Univer-

Sicherheit aus, kommen diese und wollen gern cherheit angt gehe es um frem und das sei „ga Auch and zeigten sich a WR wenig a Forscher de

Zugangscode für Gebäude entschlüsselt

Schlüsselhersteller ein generelles Verfahren der Firma Microchip als Basis für die Verschlüsselung. Die Unternehmen würden sich die Kosten für die Entwicklung eines eigenen Verfahrens sparen. Die großen Autobauer setzen zwar auf eigene Systeme. Aber, so Wi

Opel: „Natürlich ist jedes System knackbar" - Dorma: „Technik dient nur dem Komfort"

Funkschlösser für Hacker kein Problem

Von Matthias Korfmann und Klaus Bröking

Bochum. Die Nachricht schlug ein wie eine Bombe. Profi-Hacker der Uni Bochum können - wie berichtet - ganz leicht Funk-Türöffner für Autos oder Garagentore knacken. Die Autohersteller waren gestern eifrig bemüht, den Coup der Forscher kleinzureden.

„Natürlich ist jedes System knackbar. Aber wir haben noch nie Probleme gehabt. Es

hen sich mit dem Knacken der so genannten KeeLoq-RFID-Technologie beschäftigt. VW verwendet KeeLoq überhaupt nicht, also betrifft uns dieses Experiment gar nicht. Außerdem haben die Bochumer nur ein Garagentor geknackt. In unseren Autos ist schon etwas mehr Technik drin", VW-Sprecher Enrico Bel

Diesen Optim dämpft allerdings Prof nald Schöneberg von Südwestfalen in Hag gröttlich seien alle gä Funk-Schlösser leicht

cken. „Jedes System ist angreifbar, und der Schutz für die Verbraucher ist vergleichsweise gering", stellt der Experte für IT-Sicherheit fest. Dass die Schlösser relativ leicht geknackt werden können, habe etwas mit dem Kostendruck zu tun. „Bei der Herstellung kommt es oft auf we

es ein paar Ziffern mehr. Aber wer wirklich sicher gehen will, der braucht ein System mit 500 bis 1000 Ziffern, und das wollen sich die Hersteller nicht leisten", so Schöneberg.

Mechanische Schlüssel sicherer

Funk öffnen kann, dienen nicht der Sicherheit, sondern dem Komfort für die Besitzer", so Axel Schmidt, Leiter des Produktmanagements Sicherheitstechnik beim Ennepetaler Spezialisten Dorma. Er sei eigentlich „noch nie ein großes Problem gewesen", die Signale aufzufangen und zu entschlüsseln. „Je komplizierter das System ist, desto mehr macht es Professoren an den Hackern Spaß,

WESTFÄLISCHE RUNDSCH

SÜDWEST PRESSE

NEUE WÜRTTEMBERGISCHE ZEITUNG

nbrecher Aufwand zu groß

hungen sind kaum zu knacken

gen mit Funkfernbe- ufnahmen. Nach Angabundes Autoreise- und besteht kaum Gefahr, zum Öffnen der Ga- nbrechern geknackt d betonte, zwar sei r Universität Bo- iger Arbeit gelun-

gen, den Code eines der meistverwendeten Verschlüsselungssysteme zu knacken.

Doch für normale Einbrecher sei der Aufwand viel zu groß. Wer die Arbeit der Wissenschaftler nachahmen wolle, brauche mindestens einen guten Ingenieurstudenten, hochwertige Analysege-

räte, sowie vier bis sechs Monate Zeit. AP

a-reading boffins jimmy keyless door to entire universe

The Register

Biting the hand that feeds IT

United Kingdom

metro teknik

Metro, Sweden

Angriffe auf die Sicherheit

Von [redacted]

nothing to hide.

Man kennt die Szene aus der Fernseh-Werbung. Jemand zückt seinen Funkschlüssel und sämtliche Autos auf dem Parkplatz beginnen plötzlich lustig zu blinken. Ein Spaß ist das seit heute nicht mehr.

Für Militärs ist es ein Albtraum ... Kommunikation ... gemacht werden, ebenso für Banken. Aber auch der medizinische Bereich, die Produktion, der Flugverkehr oder die private Kommunikation sind mögliche Ziele für Hacker. Von der Sicherheit der Datennetze ist die moderne Gesellschaft abhängig.

Der erfolgreiche Ha-

ck Microchip car immobilizer system

Din bil kan hackes

Tysk professor beviser, at signalerne fra bilnøgler kan opfanges og kopieres, så man kan skaffe sig adgang til bilen.

Stjæl nøglen, og du kan også stjæle bilen!

Det har været biltyves svar på, at nye biler er forsynet med stadig mere avancerede startspærrer og alarmsystemer. Derfor fortæller politikredsenes døgnrapporter om flere indbrud i huse, hvor formålet har været at finde nøglerne til den dyre bil i carporten.

Men selv uden adgang til nøglerne er det muligt at skaffe sig adgan ... muligt elektronisk at hacke sig ind i bilen. Det har professor Christof Paar ... sitetet i Bochum bevist. Du kan læse mere her. Christof Paar er også med ... d i biler.

"Ved at opfange bare to signaler kan personer, der er i besiddelse ... e dine nøgle og skaffe sig adgang til garage og bil," fortæller Christof Paar.

fpn.dk

(Denmark)

Kopiering på 100 meters afstand

Han brugte den nyeste teknologi inden for afkodning til at opfange signalerne fra bilernes nøgler og fjernbetjening til garageporten. Signalerne fra det såkaldte KeeLoq-system kan kopieres på en afstand af op til 100 meter. Dermed kan hackeren efterfølgende bryde ind i både garage og bil, selv om bilproducenter og ... næmest umulig at stjæle

..., at bil ..., selv ... krypterede radiobølger. Systemet er blandt de mest populærer s

Det lykkedes også forskerne at ændre signalerne, så bilens nøgl ikke billyveri, der var forskernes formål. Dermod ville de afprøve åbne garageportene.

Forskerne understreger, at der ikke lykkedes dem at starte bilerr

sitae m. nd catio

to steal cars with

tists crack security system of millions of cars

nightmare of the remote-control age - German scientists cracked the code of the electronic bleeper that locks and garage doors.

Ruhr University says it is now relatively straightforward to ... devices that act as the electronic keys.

Sundayherald

USA

security system, which is used by Honda, Toyota, ... unit access codes using

... consternation among the car makers ...

VG NETT

Norway

Hamburger Abendblatt

Gestest

Funk-Autoschlüssel sind

Bochum Kfz-Diebstahl leicht gemacht: Viele Funk-Autoschlüssel und Garagentoröffner lassen sich mit relativ geringem Aufwand knacken. Ein Forschungsprojekt der Universität Bochum hat nun die Schwachstellen einer ganzen Reihe der sogenannten Keeloq-Sicherheitssysteme aufgedeckt.

Erstmals geknackt wurden dabei auch die Sicherheitscodes der Automobilhersteller. Dafür, so die Experten anschließend, musste lediglich der Stromverbrauch des Mikroprozessors in den Funkschlüsseln und -fernbedienungen gemessen und ausgewertet werden. "Wir waren schockiert, wie einfach das ging", so Professor Christof Paar vom Lehrstuhl für Kommunikationssicher-

heit. Einmal offengel die Codes bei allen Türöffnern der Mark fürchten nun, dass künftig im Internet könnten.

Und dann wäre Au lich ganz einfach. aus dem Baumarkt kaschrichten Zentralverriegelun tor-Fernbedienung funktioniert auf rund 100 Metern, reich abgefangen Wer dann über fügt, kann sich Z sogar Auto oder

Let's clarify things.

Torschlusspanik

Thomas Eisenbarth, Timo Kasper, Christof Paar

iX MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

NEU!

Ha

WIRTS

Sicherheit moderner Funktüröffnersysteme

Forscher knacken den Code von A

"Schwachstelle ermöglicht aus 100 Metern Entfer

Mit "Kee ... sind nich ... Christof ... ist kein ... haben ... einer ... schaffen ... Nachricht ... zu kopie ... verschaf

3sat nano

Dass auch Kleinstc sicherheitskritische

Ra

wen? lich len wollt

Berliner Morgenpost

WISSEN

Unsichere Autoschlüssel

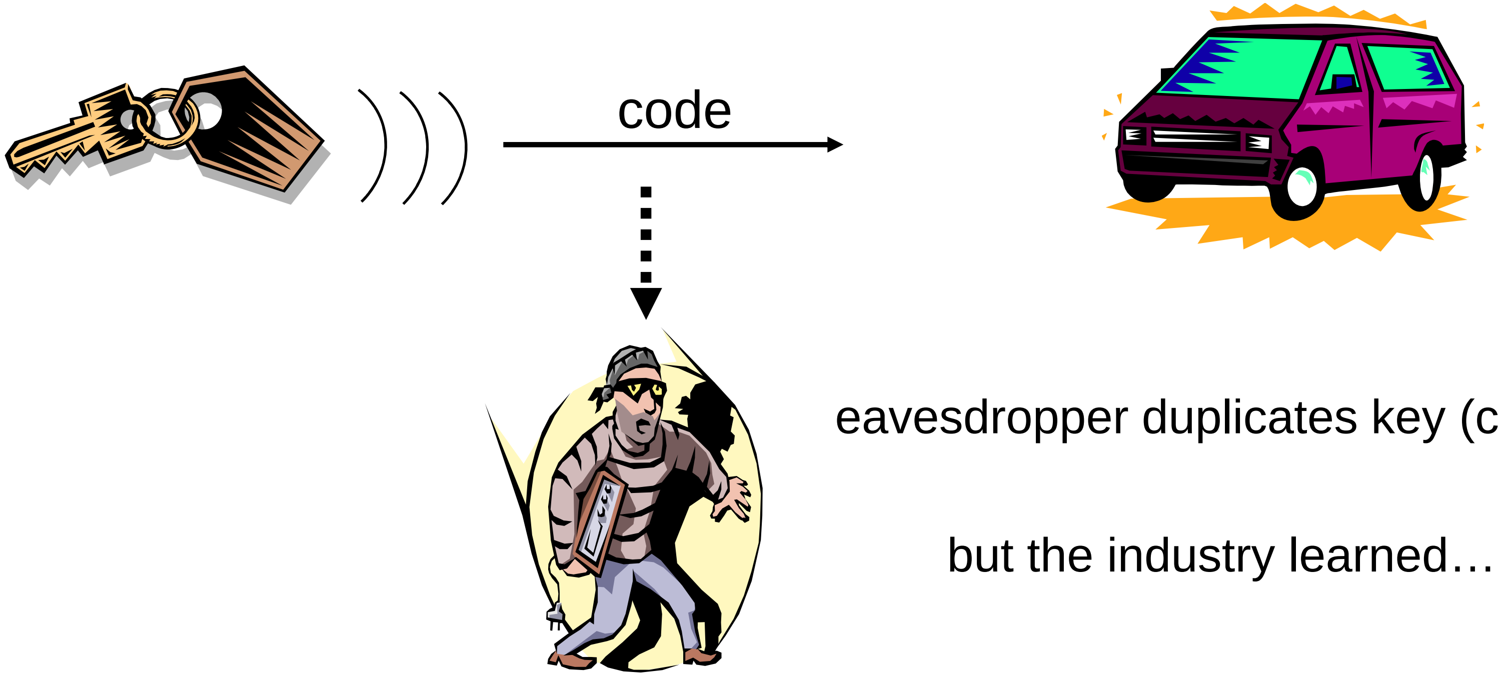
Bochum - Funkfernbedienungen für Autotüren oder Garagentore s häufig aber nicht sicher. Wissenschaftlern der Ruhr-Universität Bo eines der weltweit am häufigsten bei Funkschlüsseln verwendeten knacken und die Schlüssel aus einer Entfernung von 100 Metern z

Agenda

- Remote Keyless Entry (RKE) Systems
- KeeLoq Block Cipher
- Side-Channel Attacking KeeLoq
- Results and Implications

How do Keyless Entry Systems work?

early access controls: fixed code ("password")

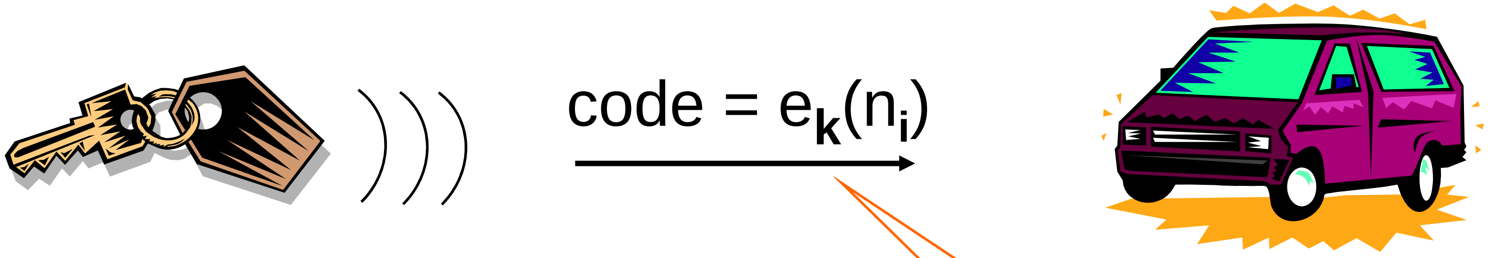


eavesdropper duplicates key (cloning)

but the industry learned…

Modern Keyless Entry Systems

advanced theft control: rolling code



code = $e_k(n_i)$

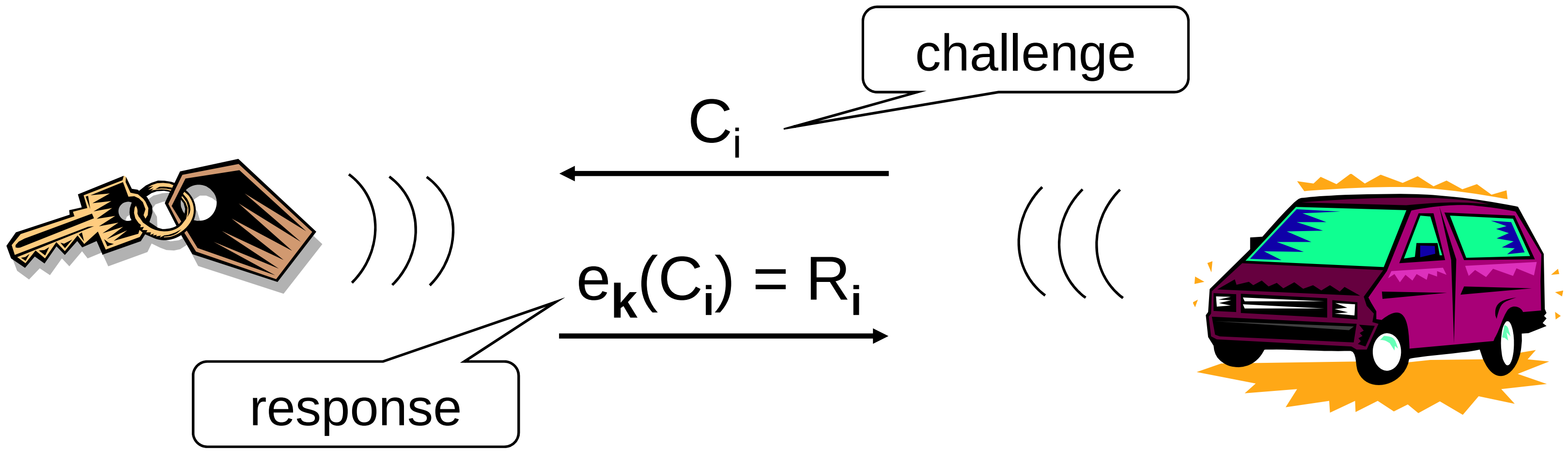
$e_k()$ is often a block cipher

rolling code (or hopping code)
protects against replay attacks:

1. code = $e_k(n)$
2. code = $e_k(n+1)$
3. code = $e_k(n+2)$

....

Alternative: Challenge - Response



challenge

C_i

$e_k(C_i) = R_i$

response

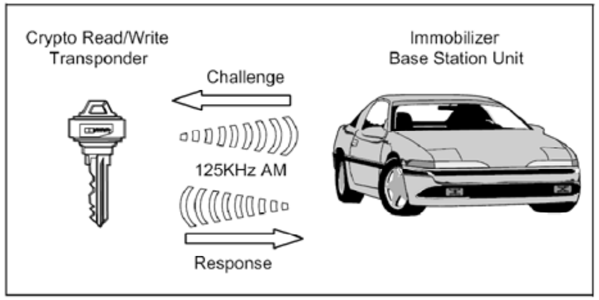
- again, $e_k()$ is often a block cipher
- also protects against replay attack
- € drawback: requires **bidirectional** devices on either side
- In most real-world car and building access control systems: rolling code

1. Computes: $R'_i = e_k(C_i)$
2. Verifies: $R'_i \overset{?}{=} R_i$

Popular Remote Keyless Entry Cipher: KeeLoq

- KeeLoq is used in rolling code mode or in a challenge-response protocol
- active remote control for access control
- KeeLoq chip embedded in passive RFID – transponder (e.g. for car immobilizer)
- Wikipedia (?): Chrysler, Daewoo, Fiat, GM, Honda, Toyota, Volvo, VW, Jaguar, ...
- widely used for **garage doors** in US & Europe

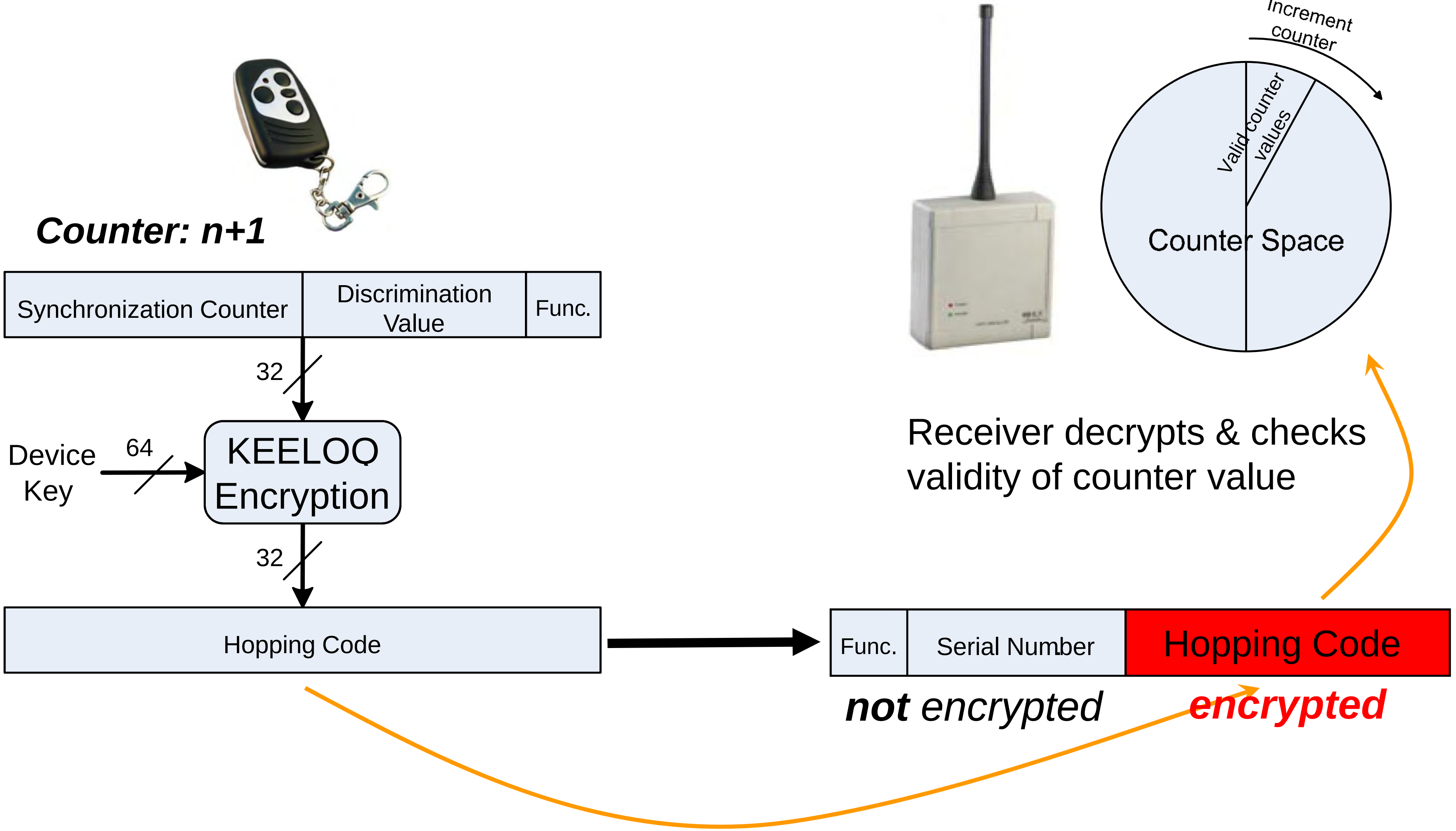
HCS410 IMMOBILIZER TRANSPONDER



KEELOQ CODE HOPPING

Q: How secure is KeeLoq?

KeeLoq Rolling Code Scheme



Counter: n+1

Synchronization Counter | Discrimination Value | Func.

32

Device Key

64

KEELOQ Encryption

32

Hopping Code

Increment counter

Valid counter values

Counter Space

Receiver decrypts & checks validity of counter value

Func. | Serial Number | Hopping Code

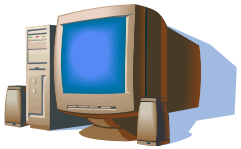
***not** encrypted*

encrypted

Key Management

OEM gets *Manufacturer Key* k_M assigned (burned in all its receivers)

1) Creation of **new remote** (in secure environment)



k_M

#ser

k_{dev} = f(#ser, $\mathbf{k_M}$)

Key derivation

2) **Key Learning Phase** of receiver
(keys are never sent in clear)

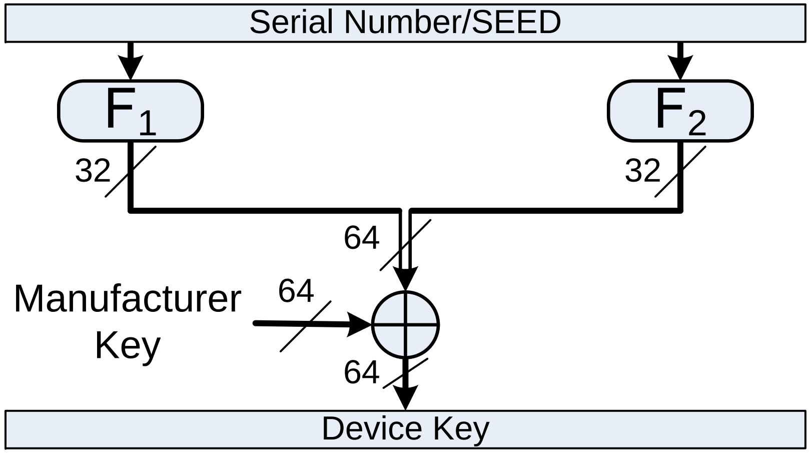
#ser

$\mathbf{k_M}$

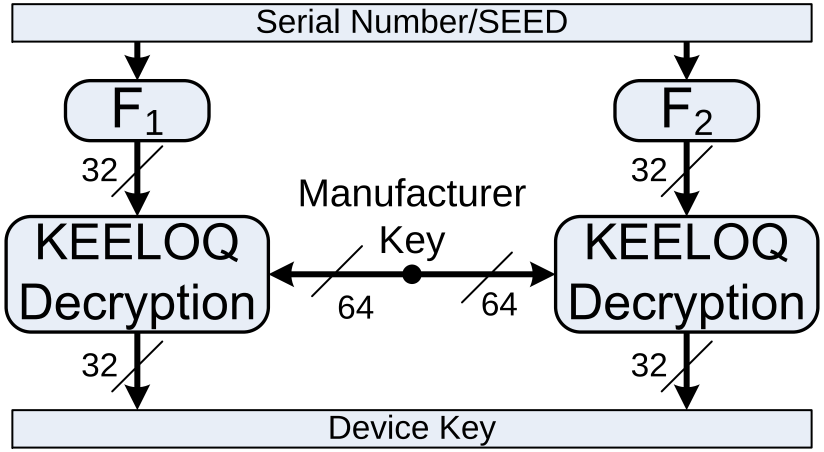
1. compute k_{dev} = f(#ser, $\mathbf{k_M}$)
2. store #ser and k_{dev}

Key Derivation Schemes

1. Weak Key Derivation (XOR)



2. Strong Key Derivation (KeeLoq)

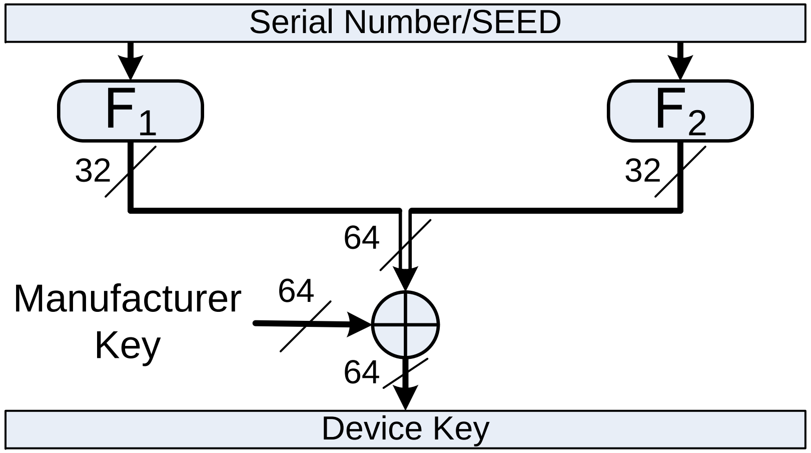


In either case, the Device Key is derived from

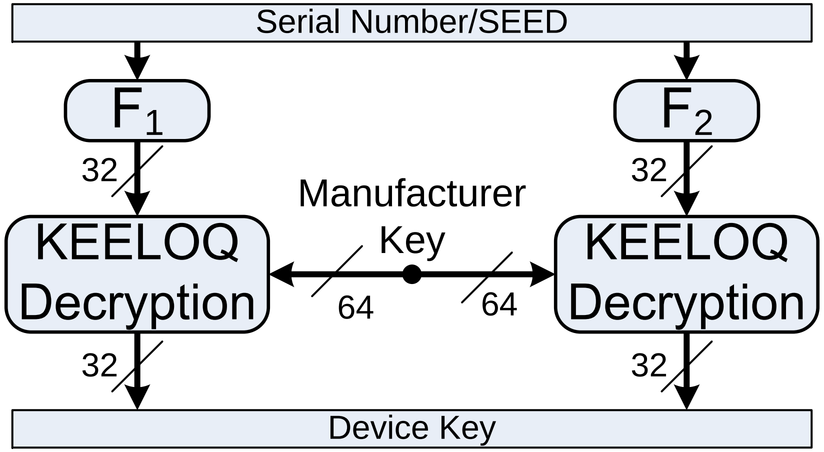
- Manufacturer key
- Serial number and/or a random seed (32…60 bits)

Key Derivation: Attacker‘s Assessment

1. Weak Key Derivation (XOR)



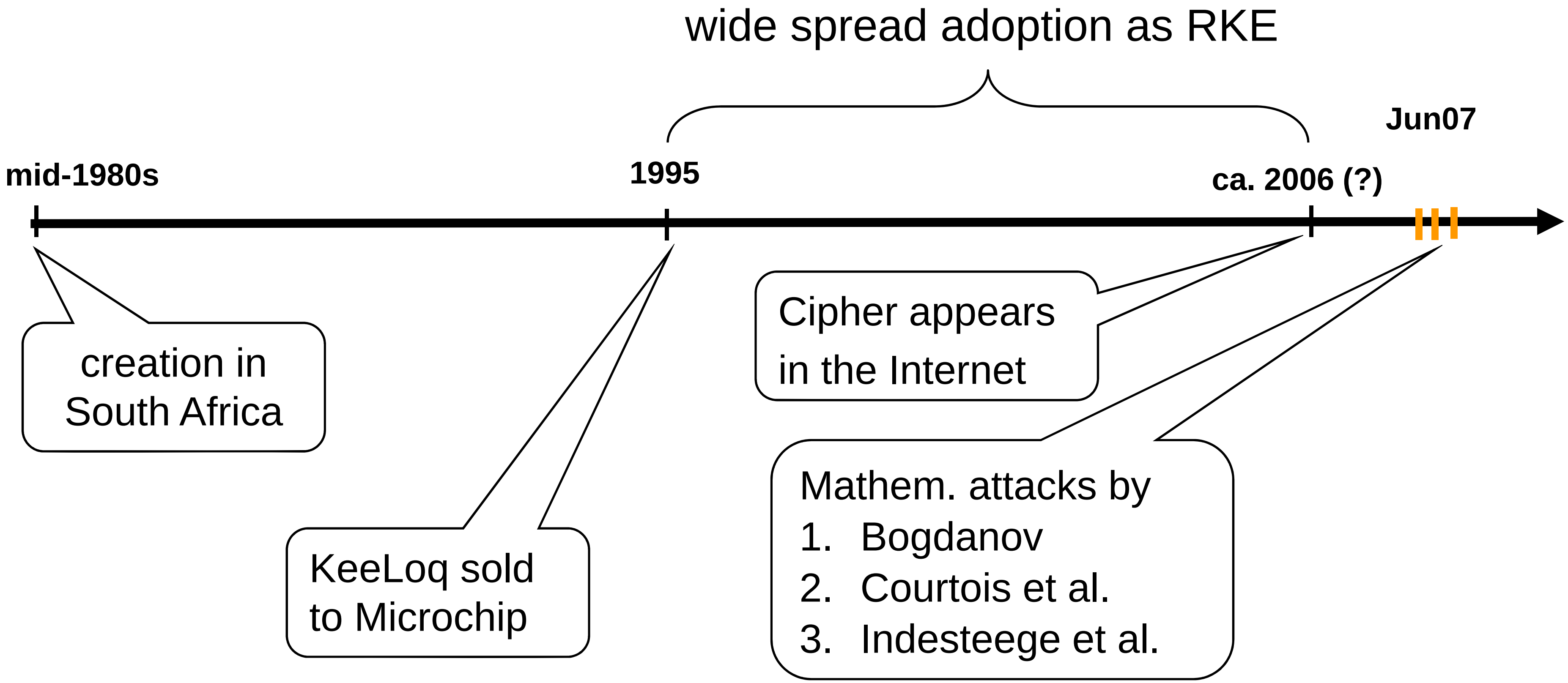
2. Strong Key Derivation (KeeLoq)



If we have the Device Key, getting the Manufacturer Key is trivial (and vice versa)

If we have the Device Key, we still have to break KeeLoq

Rise and Fall of KeeLoq



wide spread adoption as RKE

mid-1980s

1995

ca. 2006 (?)

Jun07

creation in South Africa

KeeLoq sold to Microchip

Cipher appears in the Internet

Mathem. attacks by

1. Bogdanov
2. Courtois et al.
3. Indesteege et al.

Mathematical Attacks:
Recovery of Manufacturer Key

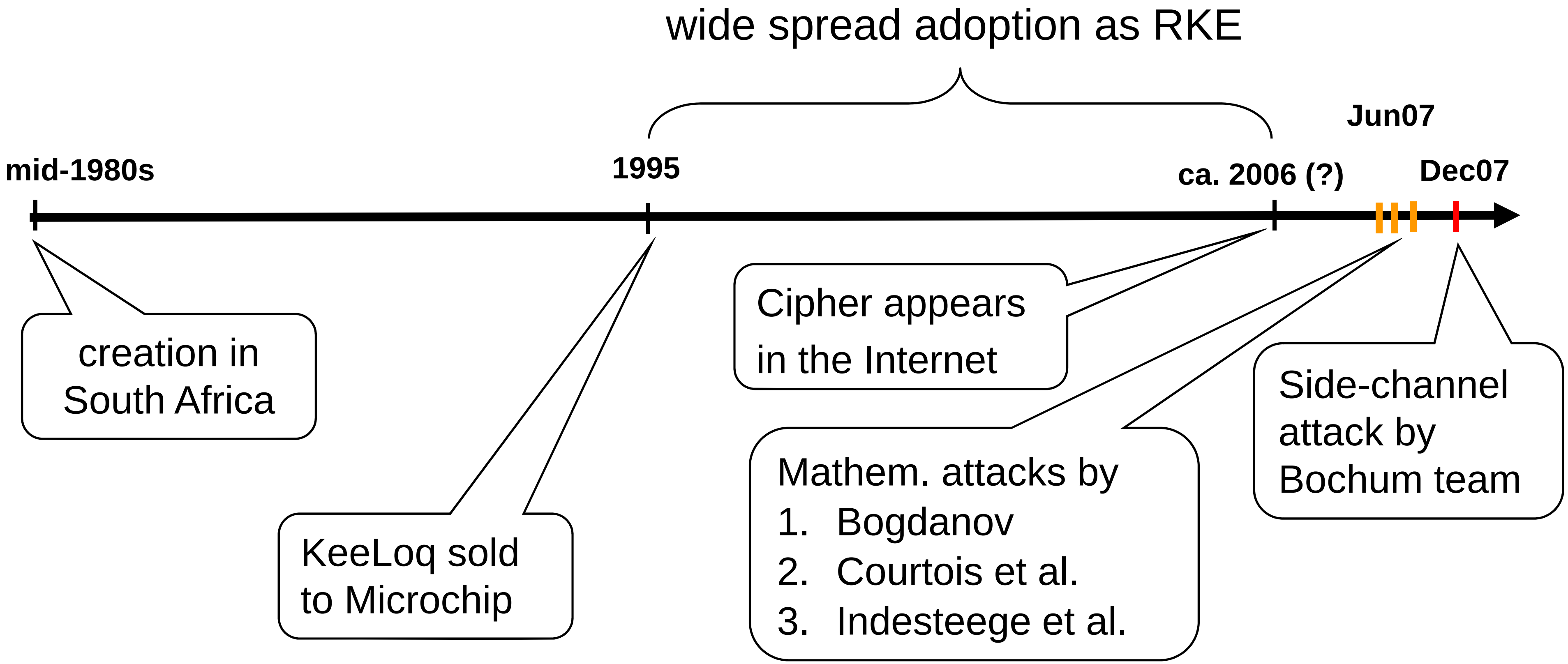
	XOR Key Derivation	KeeLoq Key Derivation
Challenge-Response	Y	N
Rolling Code	N	N

Mathematical attacks are cryptanalytically very impressive:

- Device Key is recovered from 2^{16} known plain-/ciphertext pairs
- But: Rolling code mode does **not** provide plaintext!

- **Q: How dangerous are physical attacks?**

Rise and Fall of KeeLoq



creation in South Africa

KeeLoq sold to Microchip

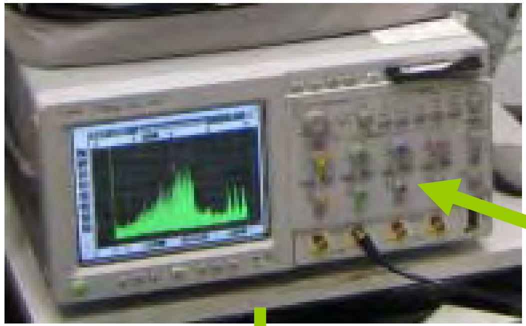
Cipher appears in the Internet

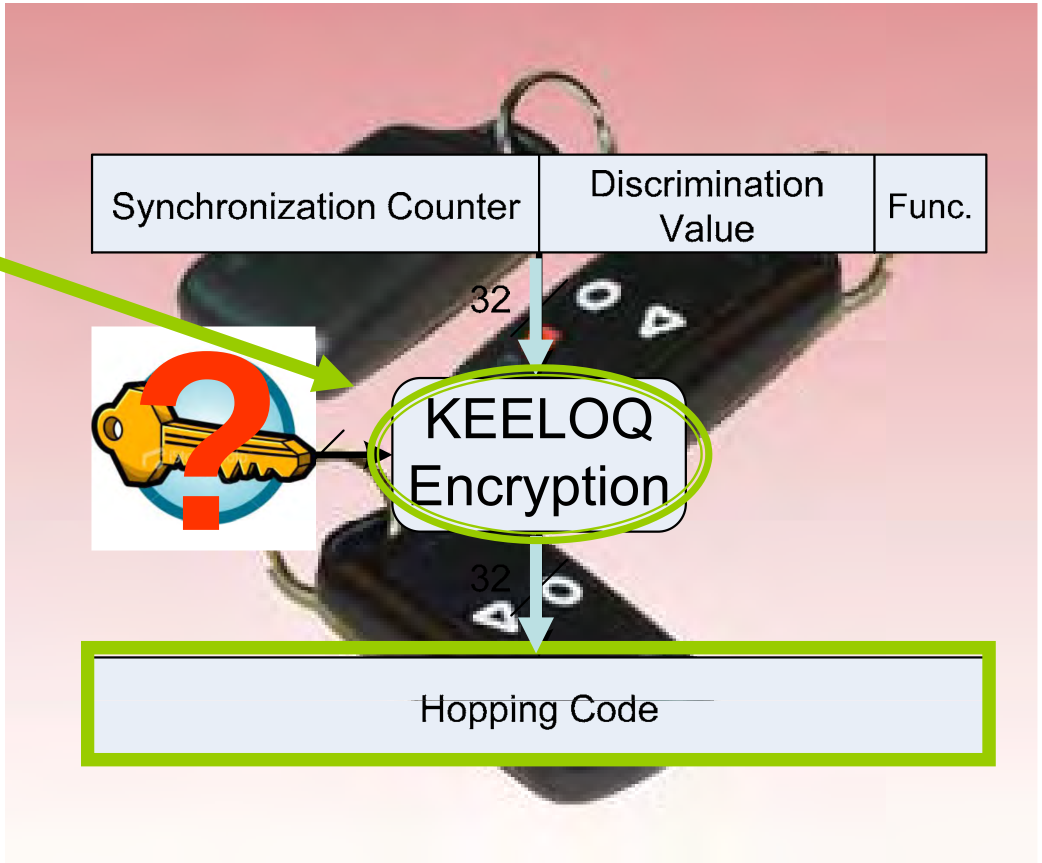
Mathem. attacks by

1. Bogdanov
2. Courtois et al.
3. Indesteege et al.

Side-channel attack by Bochum team

Power Analysis of a Remote Control





Synchronization Counter | Discrimination Value | Func.

32

KEELOQ Encryption

32

Hopping Code

secret key of remote control (HCS XXX Chip) !

History of Side-Channel Attacks (1-slide version)

- Existence of side-channels on cryptographic devices known for several decades, (e.g., “TEMPEST“)
- Few concrete results / poor understanding prior to 1996 (at least outside intelligence community)
- 2nd half of 1990s: golden years of SCA
  - Fault attack (RSA CRT), 1996
  - Timing attacks, 1996
  - SPA, DPA, 1998
- Since 1999: 100‘s of SCA research papers, e.g. in CHES
- But: so far very few (if any) documented real-world attacks