Conditional Multiple Differential Attack on MiFare Classic

or How to Steal Train Passes
and Break into Buildings Worldwide…

Nicolas T. Courtois

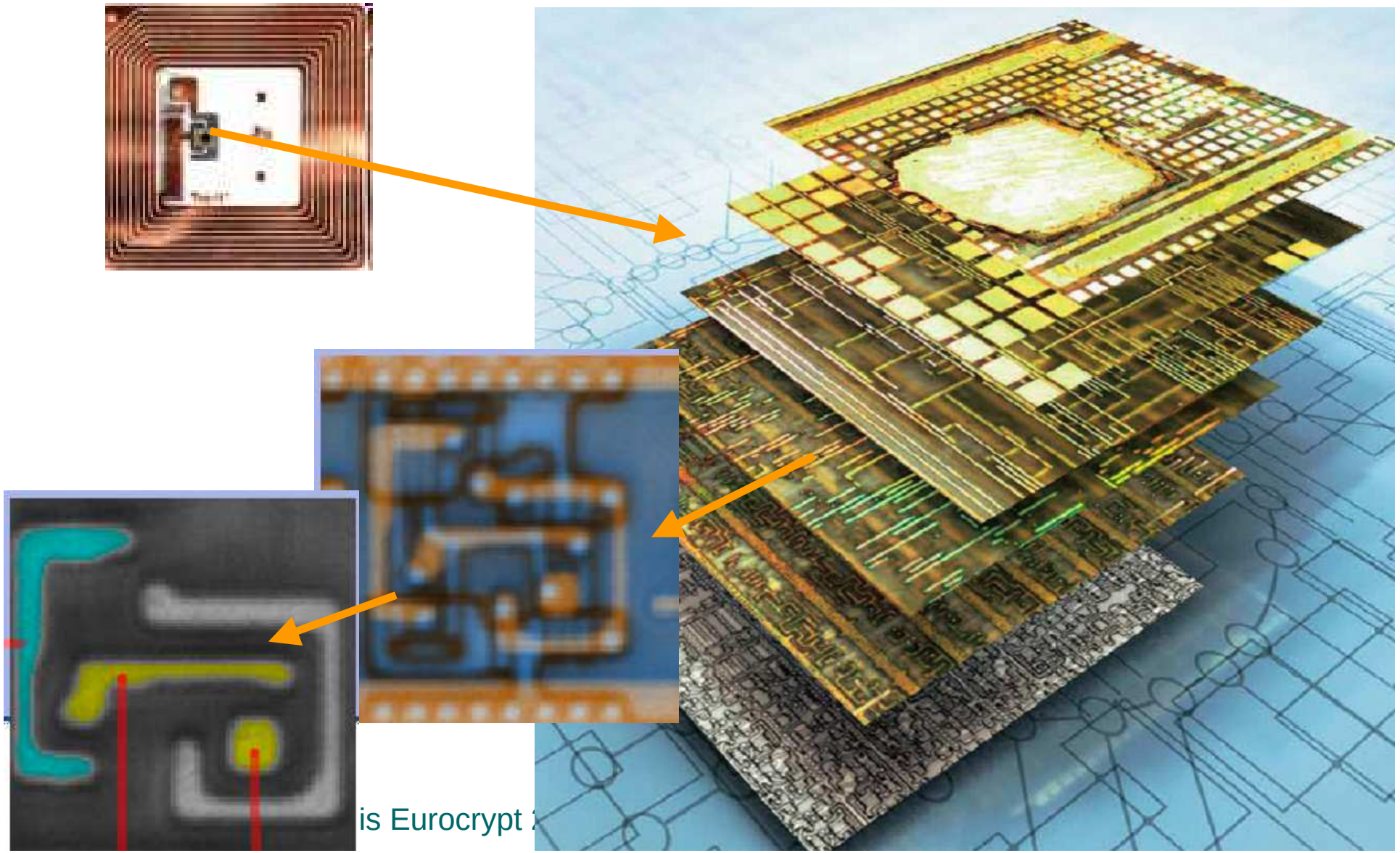
University College London, UK

MiFare Classic Crypto-1

Stream cipher used in about 200 million RFID chips worldwide.

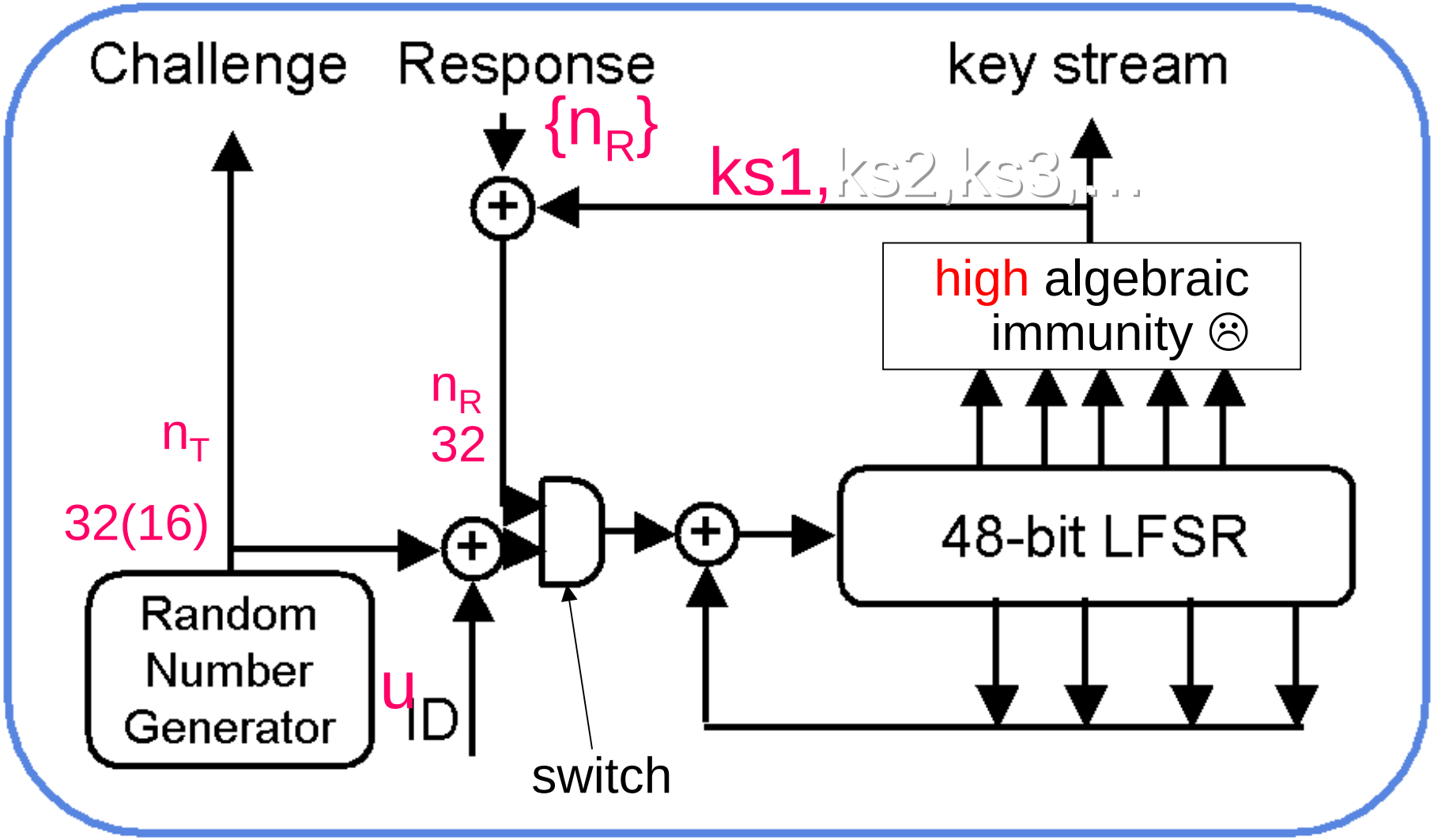
- Ticketing
  (e.g. London's Underground).
- Access to high-security buildings

Reverse-Engineering [Nohl et al.]

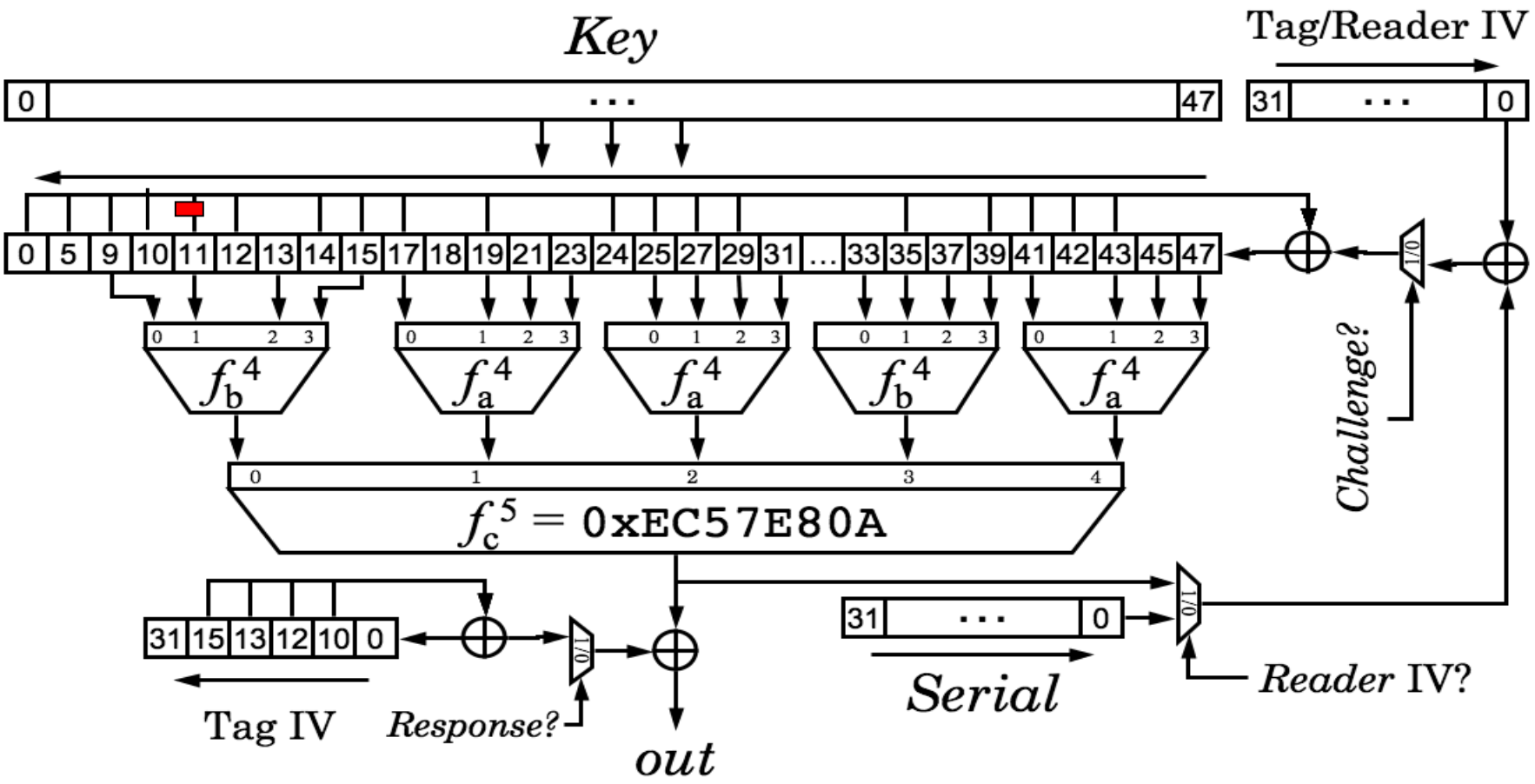


is Eurocrypt

Crypto-1 Algo + Auth. Protocol



Crypto1 Cipher



$f_a^4 = 0x9E98 = (a+b)(c+1)(a+d)+(b+1)c+a$

$f_b^4 = 0xB48E = (a+c)(a+b+d)+(a+b)cd+b$

Tag IV ⊕ Serial is loaded first, then Reader IV ⊕ NFSR

Key Recovery

with consecutive say 96 bits of keystream:

0.05 seconds.

[de Koning Gans et al, Esorics 2008]

However

These known attacks are NOT really practical.

They require access to either

- a legitimate card reader [that must know the key]
- or transcripts of recorded transactions

Hard to get in practice.

Card-Only Attacks

<u>The real security question is:</u>

Can I break it, when I am sitting near the cardholder for a few minutes in the underground (contactless card queries).

Yes, we can!

Card-Only Attacks

Danger is 24h/24:

Anybody that is sitting/standing next to you can steal your identity (or at least enter some very nice building himself…)

A Bug in MiFare Classic

Now known as parity attack.

1) the card does encrypt data with redundancy.

=> never do that…

Cf. [Biham-Barkan-Keller: Instant Ciphertext-Only Cryptanalysis of GSM.. Crypto'03 and JoC'08]

2) There is Worse…

2)

sometimes it replies
to a patient attacker with a mysterious 4 bits cryptogram…

But only sometimes. Maybe nobody would notice…

A bug or a backdoor?

Data Acquisition

Need low-level access.

These two boards + software work
and are widely available:

Open PCD

TI TRF7960 EVM

But How to Exploit This Property?

Recover the key from this scarce information???

New Nijmegen Attacks [Oakland, May 2009].
Require either

- 28500 queries to the card, or
- 4000 queries + brute-force like pre-computation + massive storage.

My attack [will be presented at SECRYPT 2009]:

- few hundred queries
- zero pre-computation
- instant running time

My Previous Attack [eprint]

A conditional multiple differential attack.

I exhibit a set of differentials that

- hold simultaneously for 256 different encryptions with overall probability of about 1/8.4
  - That ‘s a VERY high probability!
    - Source: bad bad bad Boolean functions……

```
00000001 8DC1B21F6E10
00000002 1B83643EDC20
00000004 3706C87DB840
```

See [an archived version of]: eprint.iacr.org/2009/137.

My New Attack

More dense and better.

Manipulate parity bits,
not the actual data.

We only need
a set of differentials that

- hold <u>simultaneously</u> for
  16 different encryptions
- overall probability
  of about 1/1.5

```
00000001 8DC1B21F6E10
00000002 1B83643EDC20
00000004 3706C87DB840
```

Detailed Attack

- Fix the card nonce
- Fix the 8-byte cryptogram
- Modify 8 parity bits at random until the card replies with 4-bit encrypted NACK.
  - This requires 128 queries on average.
- Now keep first 4 or more parity bits constant.
- Change the last 4 bits in the 3rd byte of the spoof cryptogram. And the last 4 parity bits too.
  - Until the card replies again.
- With probability about 1/(2*1.5)
  we get 16 encryptions with the same keystream.
  - The keystream is guessed and recovered in the attack.
- The key is then found instantly (<1 s).