Algebraic Attacks on MiFare Crypto-1, London Oyster Card, Dutch OV-Chipcard + Approx. 1 Billion other RFID Chips…

Nicolas T. Courtois [1]

Karsten Nohl [2]

Sean O'Neil [3]

[1] - University College London, UK

[2] - University of Virginia, US

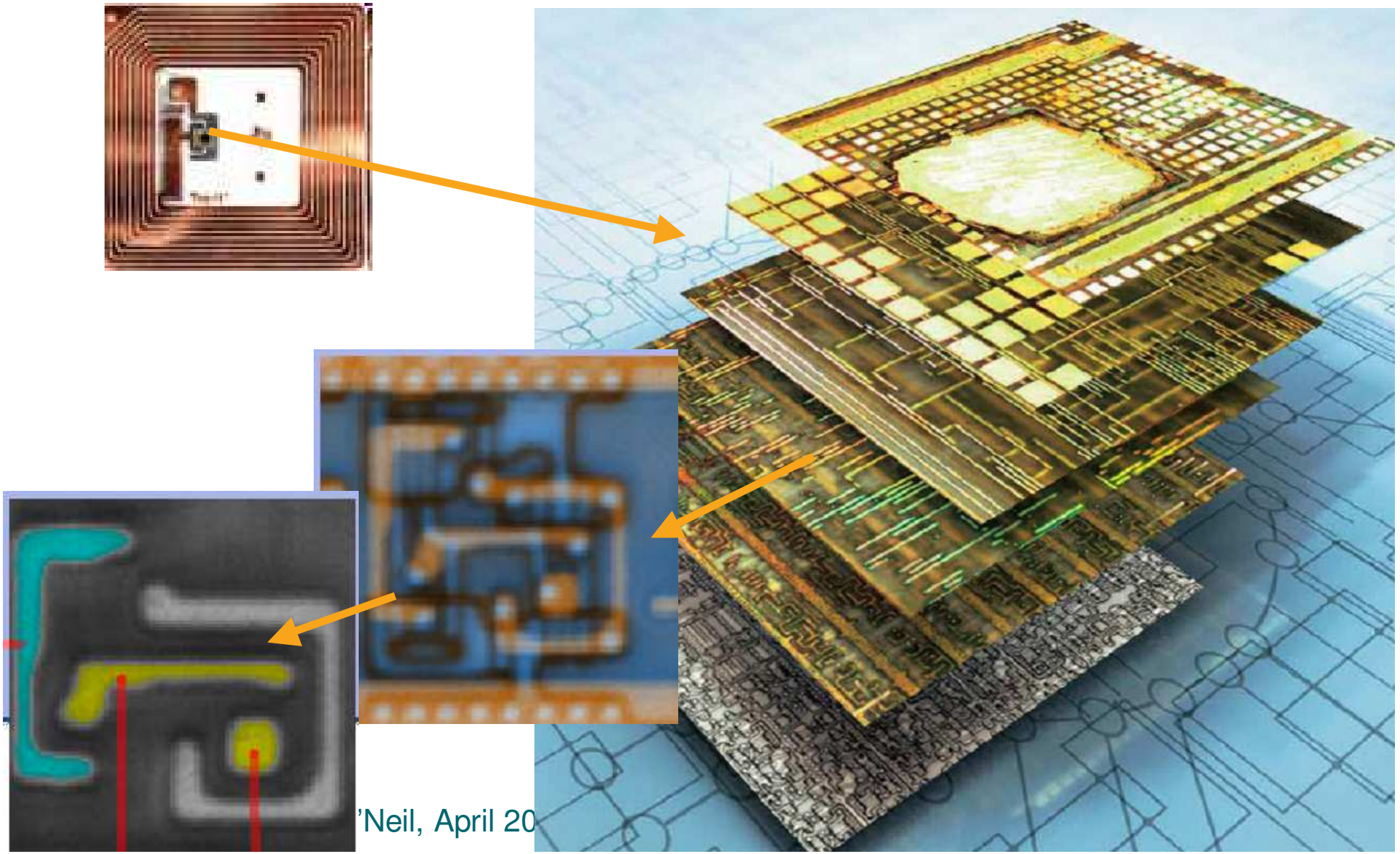
[3] - VEST Corporation, France

MiFare Classic Crypto-1

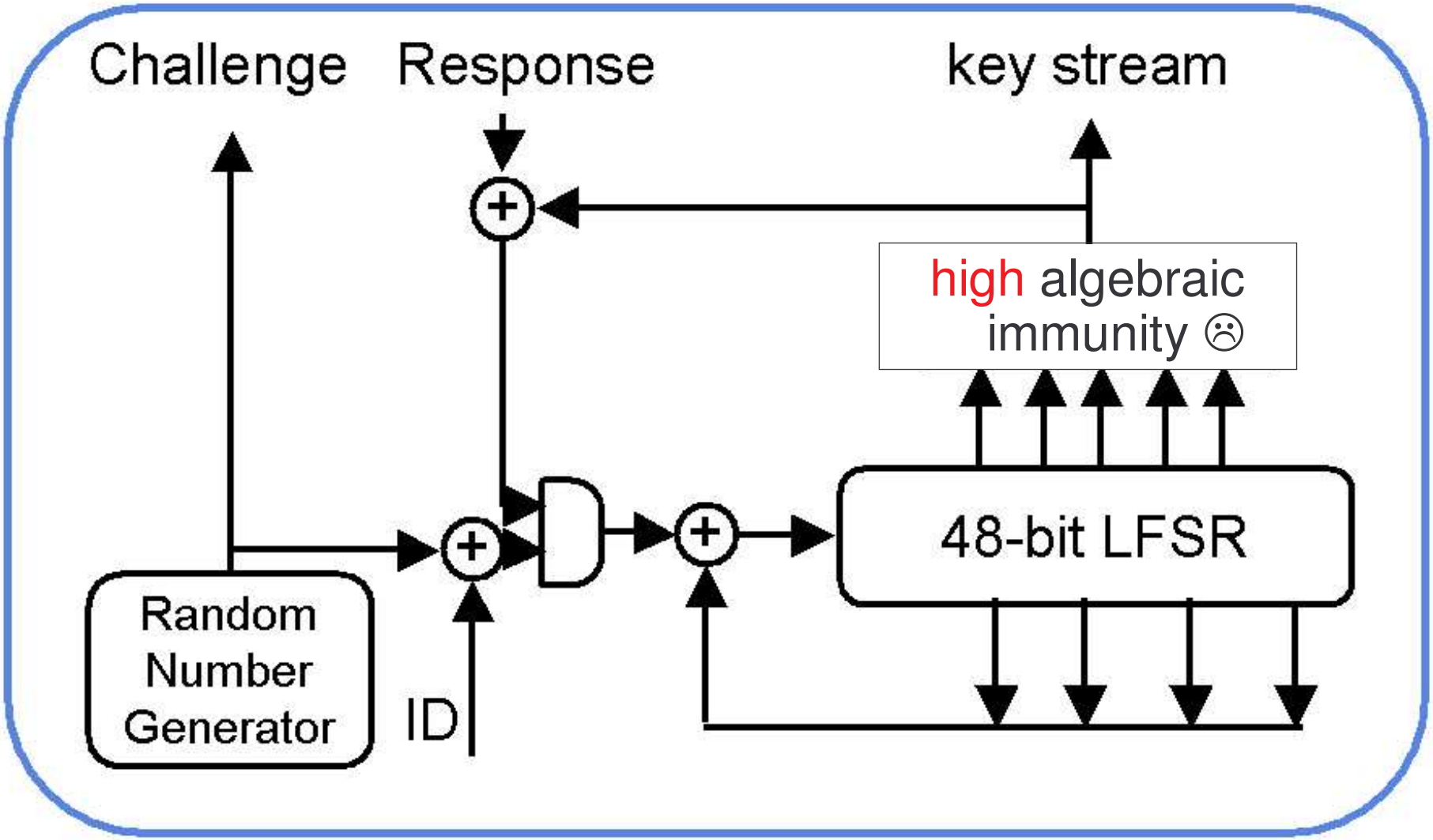
Stream cipher used in about 1 billion RFID chips worldwide.

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

Reverse-Engineering [cf. 24C3 Conf.]



MiFare Crypto-1 Algorithm

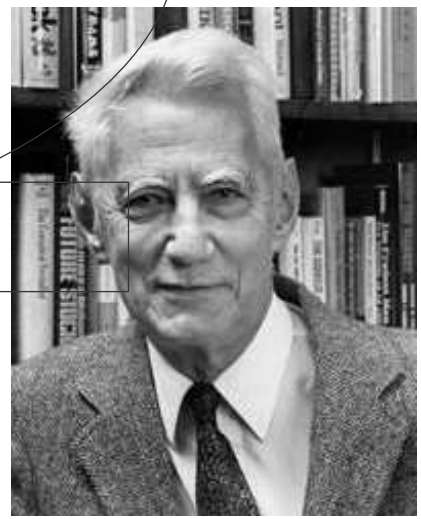


Algebraic Cryptanalysis [Shannon]

Breaking a « good » cipher should require:

"as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type"

[Shannon, 1949]



Strong or Weak?

High Algebraic Immunity.

- Does NOT help.
- Many "direct" algebraic attacks exist. We can break "any cipher", if not too complex…

Our fastest attacks use algebraic equations + conversion + SAT solvers

- [cf. recent attacks on DES and KeeLoq by Courtois and Bard 2007-08]

Exhaustive Search

- Key = 48 bits.
- Takes about 4 years
  on 1 CPU @ 1.66 GHz.

Our Algebraic Attack

- 12 seconds on the same CPU.
- Shockingly fast given the fact that 1 Billion of these chips are in use.

See eprint.iacr.org/2008/166/

There is More

What about cloning a card with:

- Passive eavesdropping
- One single transaction
- Purely cryptographic attack:
  unlike in other works on MiFare,
  we do NOT use any protocol
  or RNG vulnerability.
- Very fast, takes minutes

Preliminary results: this works.
To be published soon.