Practical Algebraic Attacks on the HITAG2™ Stream Cipher in RFID Transponders

Nicolas T. Courtois [1]

Sean O'Neil [2]

Jean-Jacques Quisquater [3]

[1] - University College London, UK

[2] - VEST Corporation, France

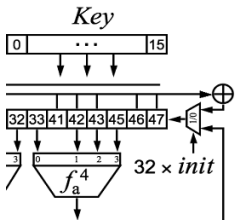
[3] - Université Catholique de Louvain, Belgium

e-Smart

Disclaimer

First of all, this pure crypto research:

Spec of the cipher => Algebraic Attack.



Not all attacks work on actual industrial systems due to the protocol subtleties.

Moreover: one should not expect that every information found on the Internet is correct. One can expect some small glitches…

Université catholique de Louvain UCL

UCL

e-Smart

Outline

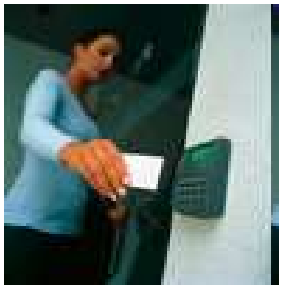
1. Hitag2 cipher and products.
2. Discussion: open source vs. closed source crypto.
3. Algebraic attacks with SAT solvers.
4. Our results.
   [Full paper published in ISC 2009, Pisa Italy, 7-9 September 2009, Springer LNCS]
5. Industry impact, discussion.

e-Smart

Hitag2

- A stream cipher used in car locks [e.g. BMW]: Philips Hitag2 family.

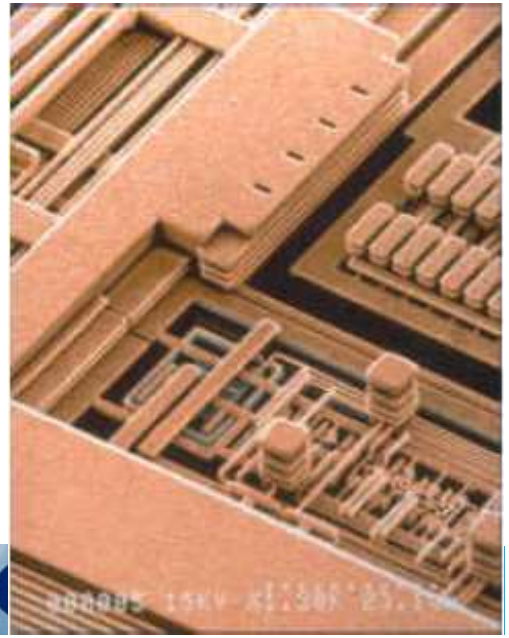
- Also used in building access.
  - According to [Nohl, Plotz HAR'09] used in German government and army buildings…
  - But Hitag2 proximity cards are not available anymore in shops. They have been discontinued.



Here we concentrate just on car locks.

e-Smart

What's Inside?



e-Smart

Open Source vs. Closed Source Crypto

e-Smart

Secrecy:

Very frequently
an obvious
business decision.

- Creates entry barriers for competitors.
- But also defends against hackers.

e-Smart

Kerckhoffs' principle: [1883]

"The system must remain secure should it fall in enemy hands …"

Université catholique de Louvain UCL

UCL

e-Smart

*Remark:

Smart Cards:

They are already in ‘enemy’ hands

- even more for RFID…

Université catholique de Louvain UCL

UCL

e-Smart

Kerckhoffs' principle: [1883]

Most of the time: incorrectly understood.

No obligation to disclose.

- Security when disclosed.
- Better security when not disclosed???

Université catholique de Louvain UCL

e-Smart

Yes (1,2,3):

1. Military:
   layer the defences.

e-Smart

Yes (2):

2)

Basic economics:

these 3 extra months

(and not more ☹)

are simply worth a

a lot of money.

Université catholique de Louvain UCL UCL

e-Smart

Yes (3):

3)

Prevent the erosion of profitability / barriers for entry for competitors / “inimitability”

Université catholique de Louvain UCL

e-Smart

Kerckhoffs principle is kind of WRONG in the world of smart cards

Reasons:

- side channel attacks are HARD and COSTLY to prevent when the algo is known
- in some applications, for example Pay TV the system is broken immediately when the cryptographic algorithms are public.

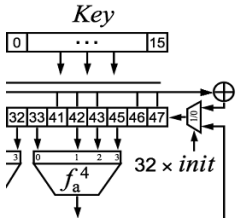
e-Smart

Kerckhoffs principle is kind of WRONG?

Well OK, but then we need other means to evaluate crypto algorithms used by the industry.

- [OLD] private consulting…
- [NEW] TODAY: Automated Cryptanalysis

Spec of the cipher => Try our software



e-Smart

Silicon Hacking

Université catholique de Louvain UCL UCL

e-Smart

Tarnovsky Lab [Freelance Silicon Hacker]

Only a few thousands of dollars worth of equipment

Université catholique de Louvain UCL

UCL

Clear and Present Danger

Reverse engineering is NOT that hard.

No need for a FIB device
(Focused Ion Beam, 0.5 M€).

A few thousand dollars microscope +software.

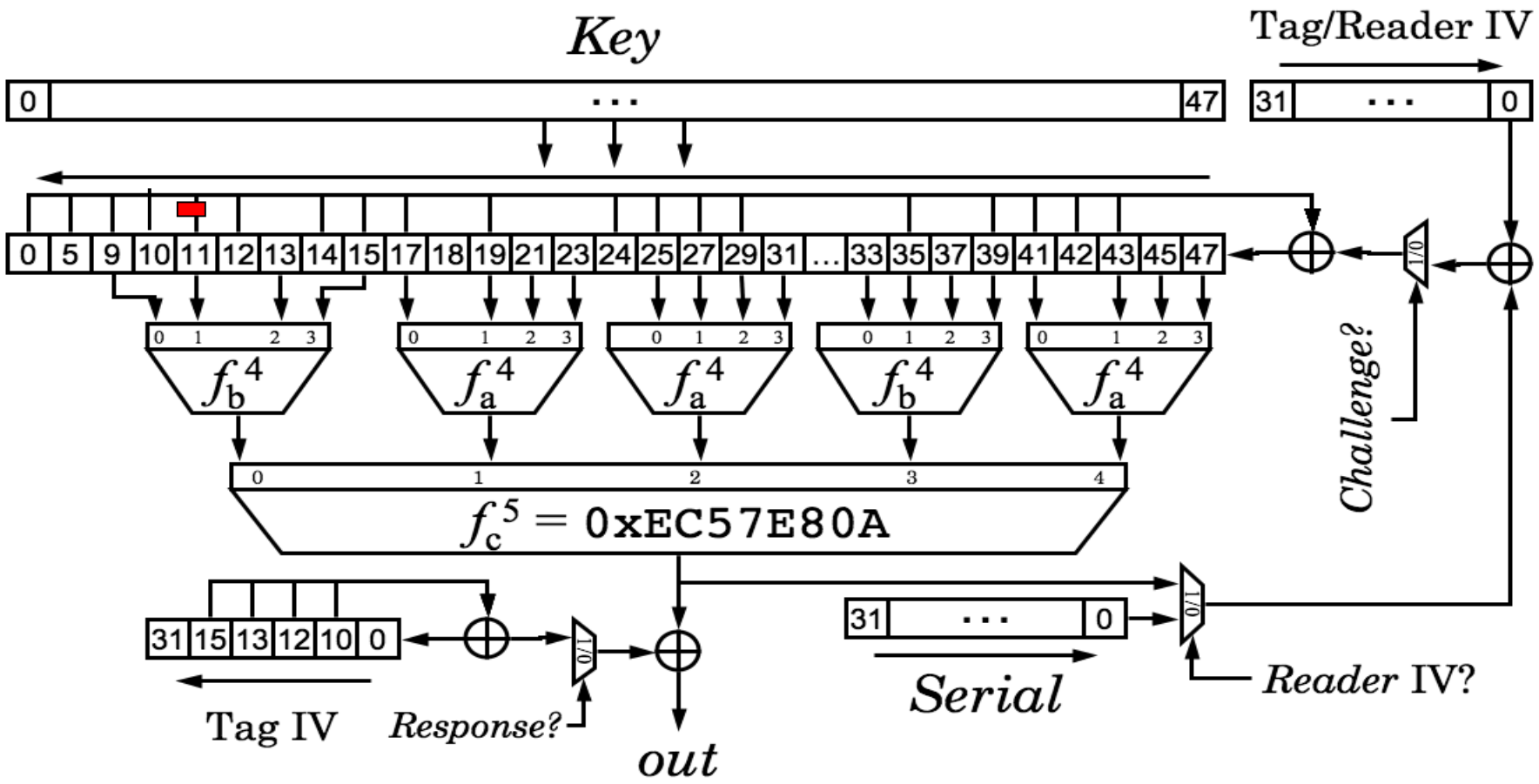
e-Smart

Silicon Hacking => Wikipedia™

Université catholique de Louvain UCL UCL

e-Smart

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

e-Smart

Crypto-1 is VERY WEAK

- Crypto 1 Has regular LFSR taps

  =>Broken in 0.05 seconds.

  [de Koning Gans et al, Esorics 2008]

e-Smart

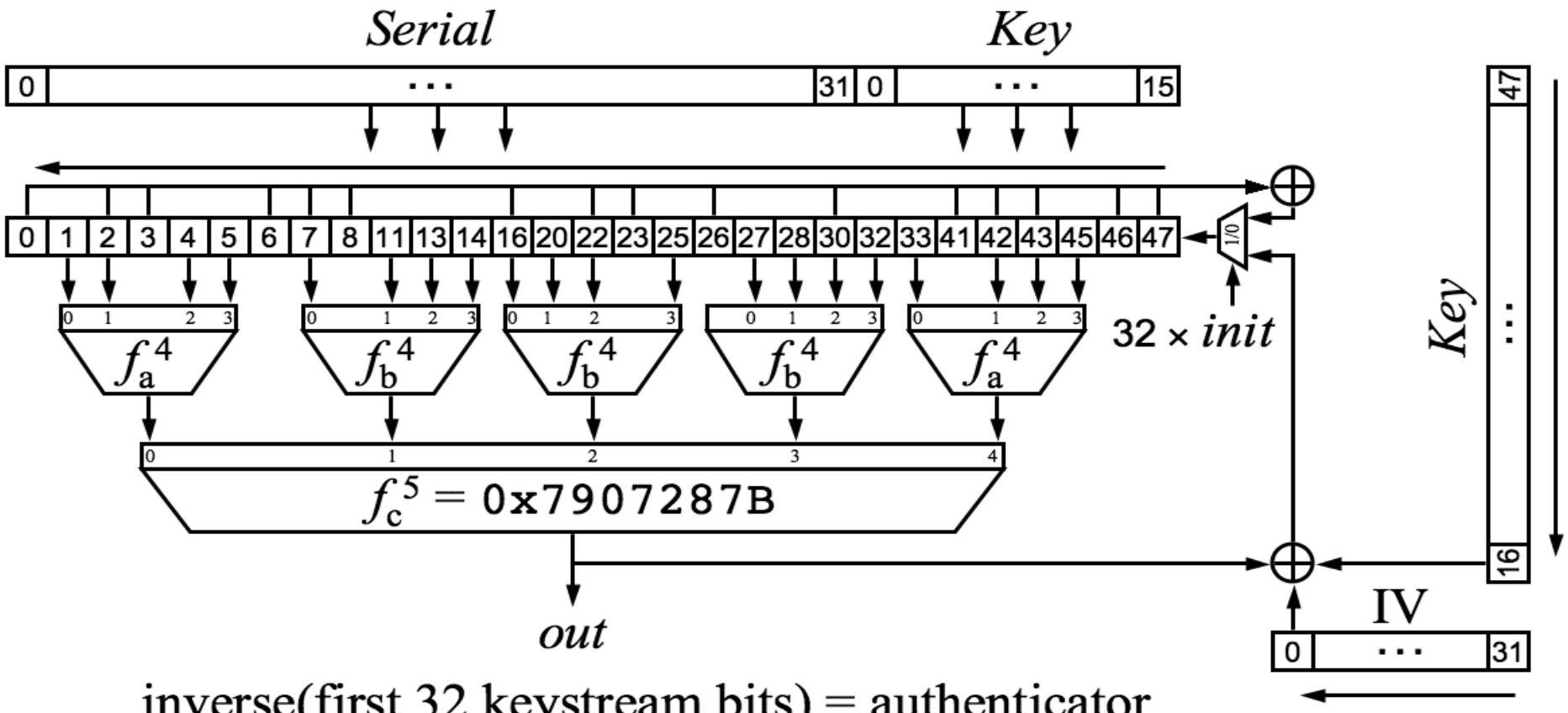
much better:

- Crypto 1 Has regular LFSR taps
  =>Broken in 0.05 seconds.
  [de Koning Gans et al, Esorics 2008]

- Hitag 2 has IRREGULAR taps. Not so easy.
- State of the art: Inversion attacks:
  - [Ross Anderson: Searching for the Optimum Correlation Attack, In FSE'94]
  - Our present work is a sort of automated inversion attack where human insights into how to invert the augmented filter function are replaced by the [clever] SAT solver software…

e-Smart

Hitag2 Cipher



inverse(first 32 keystream bits) = authenticator

$f_a^4 = 0x2C79 = abc+ac+ad+bc+a+b+d+1$

$f_b^4 = 0x6671 = abd+acd+bcd+ab+ac+bc+a+b+d+1$

e-Smart

Silicon Hacking => Wikipedia

A Cryptanalyst can start working…

Exhaustive Key Search

- 48 bits, about 4 years on 1 CPU.
  - But only hours/days with more expensive devices such as FPGA/Copacobana etc…

e-Smart

Algebraic Cryptanalysis

Université catholique de Louvain UCL UCL

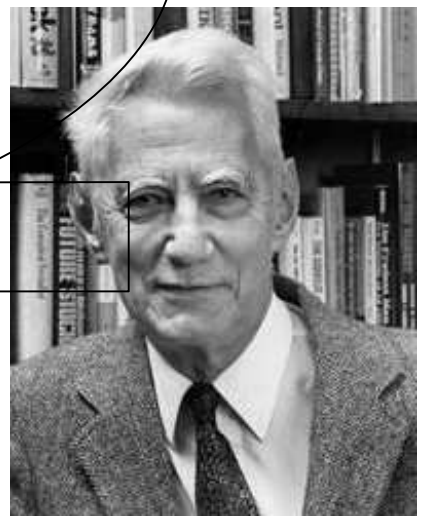
e-Smart

Algebraic Cryptanalysis [Shannon]

Breaking a « good » cipher should require:

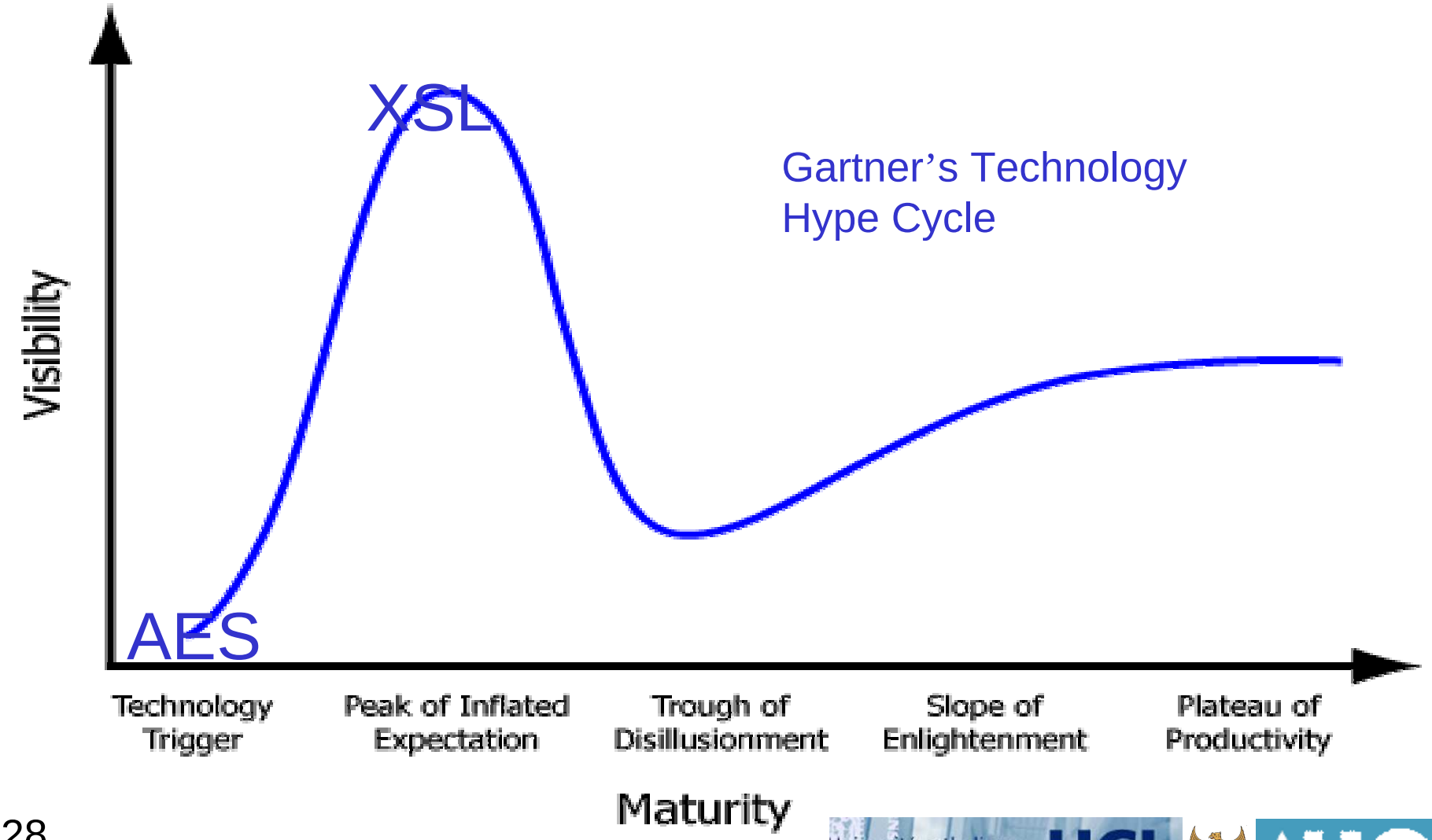
"as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type"

[Shannon, 1949]



e-Smart

Algebraic Cryptanalysis: An Emerging Technology



Courtois, O'Neil, Quisquater

Université catholique de Louvain UCL UCL

e-Smart

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

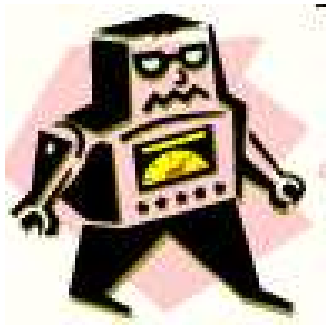
- [cf. recent attacks on DES and KeeLoq by Courtois and Bard 2007-08]

e-Smart

Our Attacks

…AC can break “any cipher”,

if not too complex…



Remark:

- Other attacks can be faster.
- However, this method is more generally applicable:
  - we can also break many modified versions of Hitag2
  - and this without any human intervention !

e-Smart

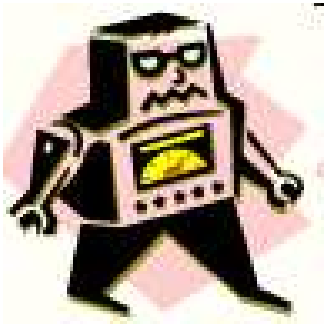
Algebraic Cryptanalysis

Step 1.

Write a system of Multivariate Quadratic equations [MQ]

Step 2.

Solve it.



e-Smart

ANF-to-CNF method - The Outsider

[Courtois, Bard, Jefferson]

Before we did try,

we actually never believed it could work…

☺ ☺ ☺

Convert MQ to a SAT problem.

(both are NP-hard problems)

*ANF-to-CNF – Main Idea

Principle 1:

each monomial = one dummy variable.

$$a = wxyz$$

$$\Updownarrow$$

$$a \iff (w \wedge x \wedge y \wedge z)$$

$$\Updownarrow$$

$$(w \vee \bar{a})(x \vee \bar{a})(y \vee \bar{a})(z \vee \bar{a})(a \vee \bar{w} \vee \bar{x} \vee \bar{y} \vee \bar{z})$$

d+1 clauses for each degree d monomial

*Also

Principle 2:

Handling XORs – Not obvious. Long XORs known to be hard problems for SAT solvers.

$$a \oplus b \oplus c \oplus d = 0$$

$$\Updownarrow$$

$$(\bar{a} \vee b \vee c \vee d)(a \vee \bar{b} \vee c \vee \bar{d})(a \vee b \vee \bar{c} \vee d)(a \vee b \vee c \vee \bar{d})$$
$$(\bar{a} \vee \bar{b} \vee \bar{c} \vee d)(\bar{a} \vee \bar{b} \vee c \vee \bar{d})(\bar{a} \vee b \vee \bar{c} \vee \bar{d})(a \vee \bar{b} \vee \bar{c} \vee \bar{d})$$

- Split longer XORs in several shorter with more dummy variables.
- About 4 h clauses for a XOR of size h.

e-Smart

*ANF-to-CNF

This description is enough to produce a working version.

Space for non-trivial optimisations. See:

Gregory V. Bard, Nicolas T. Courtois and Chris Jefferson:

“Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF(2) via SAT-Solvers”. eprint.iacr.org/2007/024

e-Smart

Solving SAT

What are SAT solvers?

Heuristic algorithms for solving SAT problems.

- Guess some variables.
- Examine consequences.
- If a contradiction found, I can add a new clause saying “In this set of constraints one is false”.

Very advanced area of research.

Introduction for “dummies”:

Gregory Bard PhD thesis.

MiniSat 2.0.

Winner of SAT-Race 2006 competition.

An open-source SAT solver package,
by Niklas Eén, Niklas Sörensson,

http://www.cs.chalmers.se/Cs/Research/FormalMethods/MiniSat/

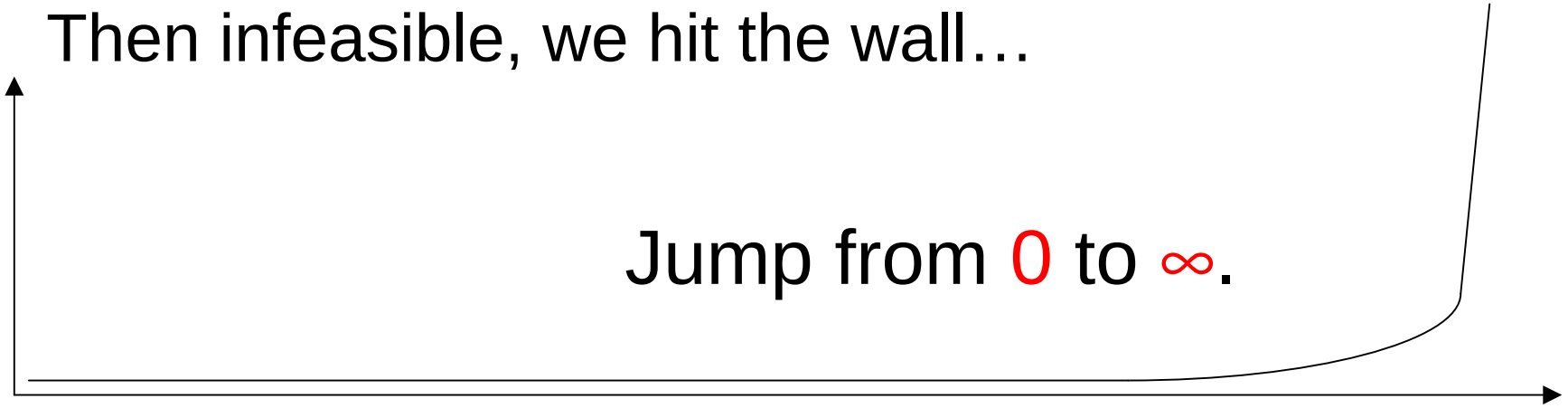
Compiles with gcc under both Unix and Windows.

e-Smart

**ANF-to-CNF + MiniSat 2.0.

Gives amazing results in algebraic cryptanalysis of just any (not too complex/not too many rounds) cipher. Also for random sparse MQ.

- Certain VERY large systems solved in seconds on PC (thousands of variables !).
- Few take a couple hours/days…
- Then infeasible, we hit the wall…



**What Can Be Done with SAT Solvers ?

- Clearly it is not the size of the system but the nature of it.
- Sometimes more powerful than Grobner Bases, sometimes less.

Paradoxes:

- If you guess some variables, can become much slower ☺.
- Great variability in results (hard to compute an average running time, better to look at 20 % faster timings).
- Memory:
  - For many cases tiny: 9 Mbytes while Magma hangs at > 2Gbytes for the same system.
  - For some working cases: 1.5 Gbytes and substantial time. Then terminates with the solution as well.

e-Smart

Hitag2 Protocols

From Original Philips Specs

- Found on a Russian web side(!)
- Hitag 2 have two modes.
  - Password mode [less secure]
  - Crypto mode.

- We focus on the crypto mode.

Sort of challenge-response protocol.

  - Mutual authentication.
  - But the reader is authenticated first.
    - Prevents tag-only attacks, or attacks at home:
      - sniffed data is needed.

e-Smart

Mutual Authentication in the Crypto mode

- The tag sends:

$$11111 + SN \longrightarrow$$

5 +32 bits

- The car picks a random IV (32 bits) and sends:

$$IV + ks1 \longleftarrow$$

32 + 32 bits

- If the stream authenticator ks1 is correct, tag sends

$$11111 + (Config||PWST) \oplus ks2 \longrightarrow$$

5 + 32 bits

where PWST is a password, ks1,ks2 are the first 32+32 bits of Hitag 2 keystream initialised with (K,IV)

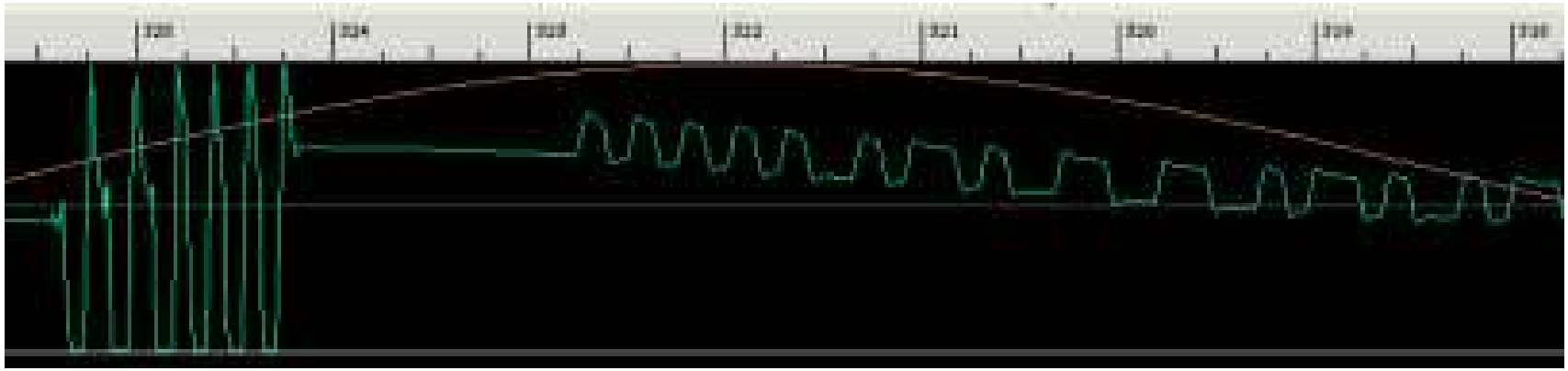
e-Smart

Sniffed Traces?

We did not do the actual hacking of car keys.

Some recorded Hitag2 traces
can be found in [Nohl, Plotz HAR'09]

https://har2009.org/program/attachments/113_breaking_hitag2_part1_hardware.pdf



e-Smart

Our Results

Our Chosen IV Attack [not practical]

NOT practical.

- An active attacker can send the data to the tag, but the tag will NOT respond if the authenticator is incorrect…
- Purely theoretical attack:
  - We need to know the ks1 for 16 authentication attempts with 16 chosen IVs in the counter mode (consecutive integers on 32 bits).
  - We combine 16 systems of equations. We don't guess any bits.
  - The complete 48-bit key is then found in 6 hours on a PC with MiniSat 2.0.
- The full attack is 6 hours total.

e-Smart

Our Known IV Attack [practical !]

This attack slower BUT it is practical given the protocol:

- Sniffed data from 4 transactions needed.
- 32 bits of the keystream per known IV are available (assuming PWST is already known).
- We fix/guess 14 bits of the key and combine 4 systems of equations for 4 known IVs.
  - The solution is then found in 10 seconds on a PC with MiniSat 2.0.
- The full attack on a full 48-bit key takes about

$2^{14}*10$ s which is less than 2 days.

e-Smart

Cryptanalysis and the Industry

Industry Impact?

"old" industry:

- Good excuse to replace these old systems.
  - Nobody thought they would be very secure by today's standards…

"new" industry:

- Silicon hacking labs: we need to realize that:

  $\Rightarrow$ what people in Europe/US do so that they can evaluate the security of the product (and publish a nice paper)…,

  $\Rightarrow$ it will be done routinely in China and by several firms
  BUT not for research, but for the manufacturing industry
  (and it will be legal: in Chinese law),

e-Smart

*Example, cf. made-in-china.com:

Supports:

Mercedes,

BMW

e-Smart

*Programmer 2: [All come from China]

Supports: BMW
(2002 -2009)

CAS/CAS2/CAS3
DG512 / CAS3 +
DP512 key and
remote control

Université catholique de Louvain UCL

UCL

e-Smart

*Programmer 3: [China]

Audi A8, VW Touareg, VW Phaeton, Bentley Continental, Porsche Cayenne, BMW

E38, E39, E46, E53, E60, E61, E63, E64, E65, E66, E87, E90, E91, E92

Université catholique de Louvain UCL

UCL

e-Smart

*Programmer 4: [China]

Audi A8, VW Touareg,
VW Phaeton,
Bentley Continental,
Porsche Cayenne,
BMW
E38, E39, E46, E53,
E60, E61, E63, E64,
E65, E66, E87, E90,
E91, E92

e-Smart

*Programmer 5: [China]

Audi A8, VW Touareg,
VW Phaeton,
Bentley Continental,
Porsche Cayenne,
BMW
E38, E39, E46, E53,
E60, E61, E63, E64,
E65, E66, E87, E90,
E91, E92

Université catholique de Louvain UCL

UCL

Conclusion

Old industrial ciphers can now be routinely broken by automated tools such as SAT solvers.

The industry needs to recognise that:

- Reverse engineering is cheaper and easier than ever. A microscope + software…
- "Kindegarten crypto" fails.

e-Smart

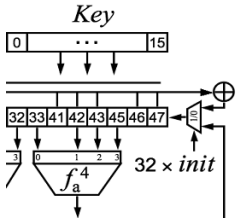
New Perspective for the Industry

- Old / Kindegarten crypto fails.
- Custom/secret crypto is OK.
  - But it needs to be evaluated and tested.

We propose a new method to evaluate crypto algorithms used by the industry.

- [OLD] private consulting…with selective disclosure.
- [NEW] TODAY: Automated Cryptanalysis

Spec of the cipher => Try our software



no need to DISCLOSE the SPEC!

Université catholique de Louvain UCL