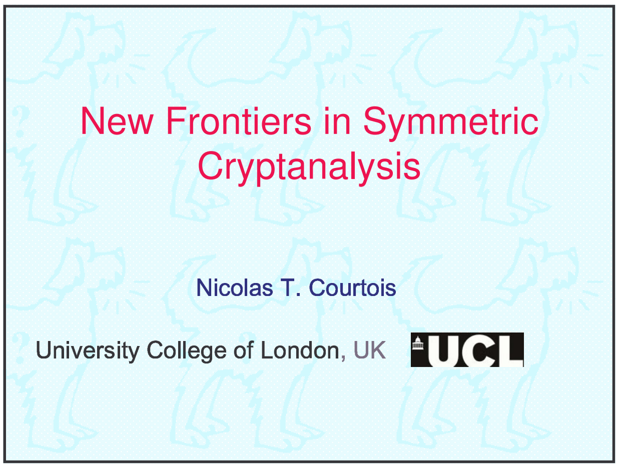
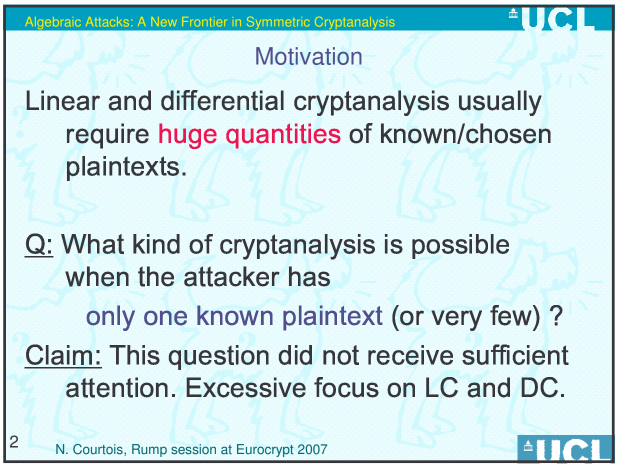


New Frontiers in Symmetric Cryptanalysis

Nicolas T. Courtois

University College of London, UK



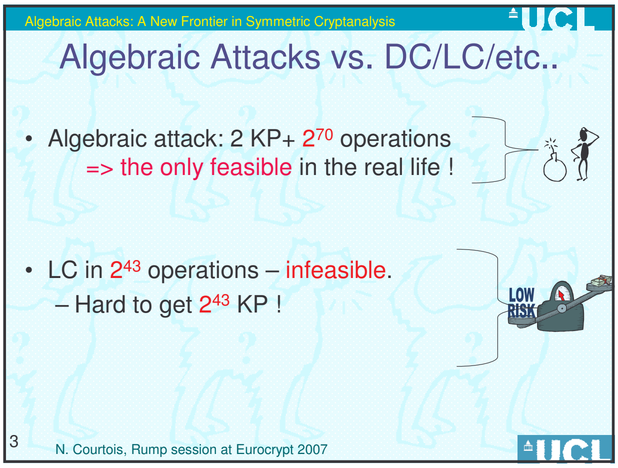
Motivation

Linear and differential cryptanalysis usually require huge quantities of known/chosen plaintexts.

Q: What kind of cryptanalysis is possible when the attacker has

only one known plaintext (or very few) ?

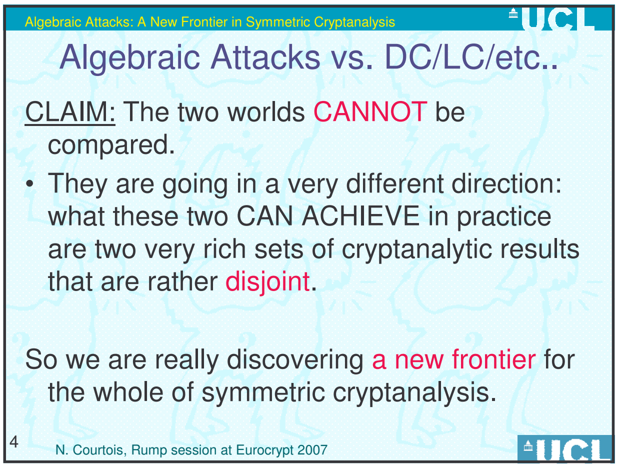
Claim: This question did not receive sufficient attention. Excessive focus on LC and DC.



Algebraic Attacks vs. DC/LC/etc..

- Algebraic attack: 2 KP+ 2^{70} operations
  => the only feasible in the real life !

- LC in 2^{43} operations – infeasible.
  - Hard to get 2^{43} KP !

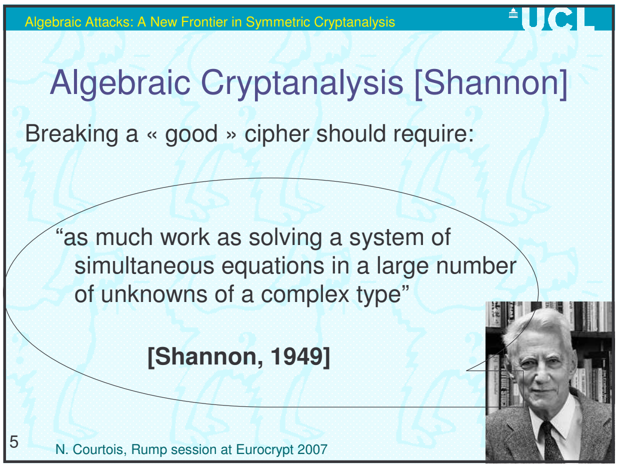


Algebraic Attacks vs. DC/LC/etc..

CLAIM: The two worlds CANNOT be compared.

- They are going in a very different direction: what these two CAN ACHIEVE in practice are two very rich sets of cryptanalytic results that are rather disjoint.

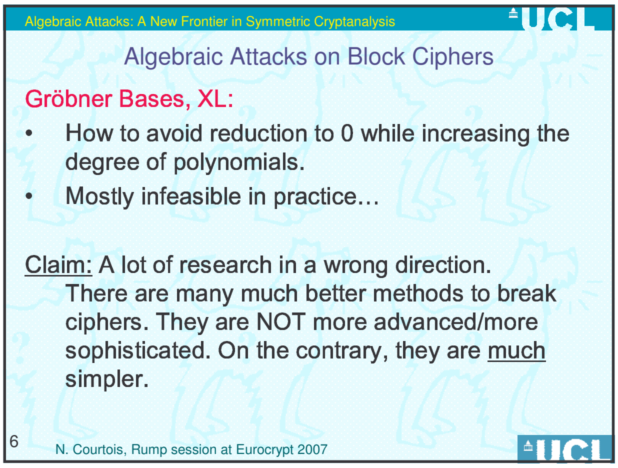
So we are really discovering a new frontier for the whole of symmetric cryptanalysis.



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]**

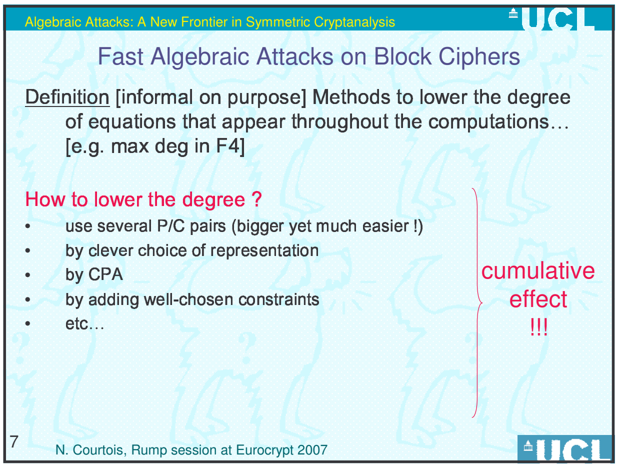


Algebraic Attacks on Block Ciphers

Gröbner Bases, XL:

- How to avoid reduction to 0 while increasing the degree of polynomials.
- Mostly infeasible in practice…

Claim: A lot of research in a wrong direction. There are many much better methods to break ciphers. They are NOT more advanced/more sophisticated. On the contrary, they are much simpler.



Algebraic Attacks: A New Frontier in Symmetric Cryptanalysis

Fast Algebraic Attacks on Block Ciphers

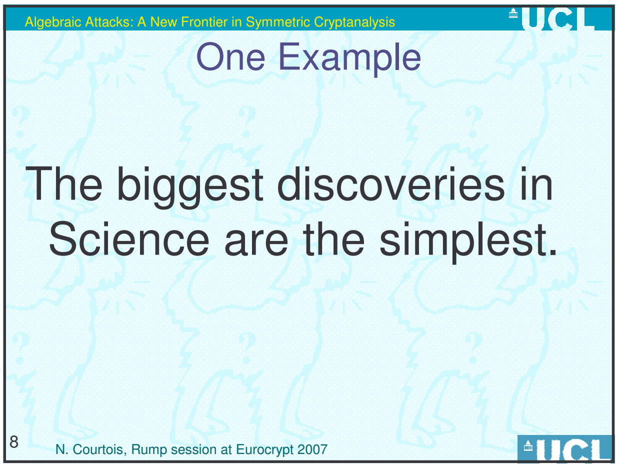
Definition [informal on purpose] Methods to lower the degree of equations that appear throughout the computations… [e.g. max deg in F4]

How to lower the degree ?

- use several P/C pairs (bigger yet much easier !)
- by clever choice of representation
- by CPA
- by adding well-chosen constraints
- etc…

cumulative effect !!!

7 N. Courtois, Rump session at Eurocrypt 2007

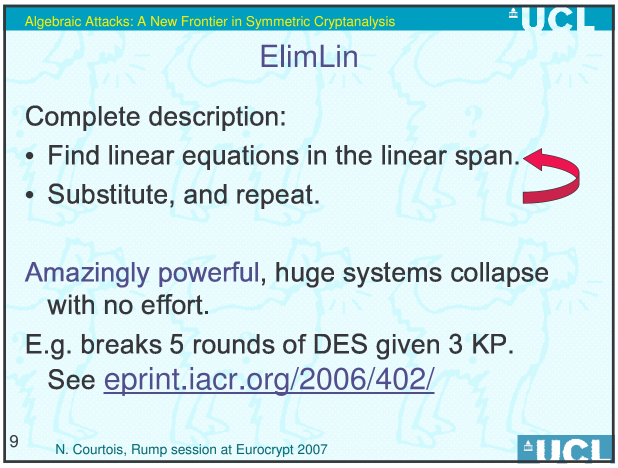


Algebraic Attacks: A New Frontier in Symmetric Cryptanalysis

One Example

The biggest discoveries in Science are the simplest.

8 N. Courtois, Rump session at Eurocrypt 2007



Algebraic Attacks: A New Frontier in Symmetric Cryptanalysis

ElimLin

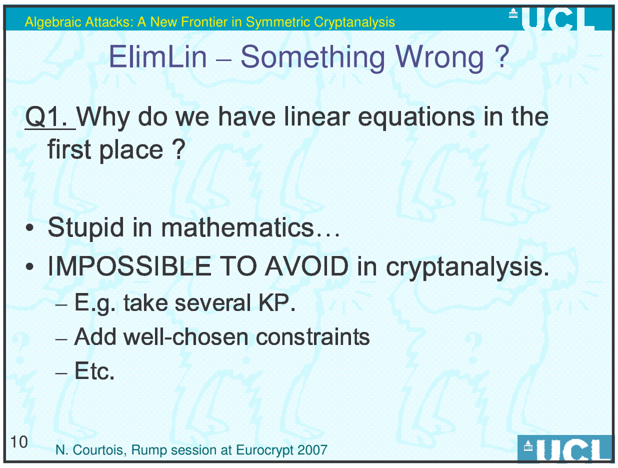
Complete description:

- Find linear equations in the linear span.
- Substitute, and repeat.

Amazingly powerful, huge systems collapse with no effort.

E.g. breaks 5 rounds of DES given 3 KP. See eprint.iacr.org/2006/402/

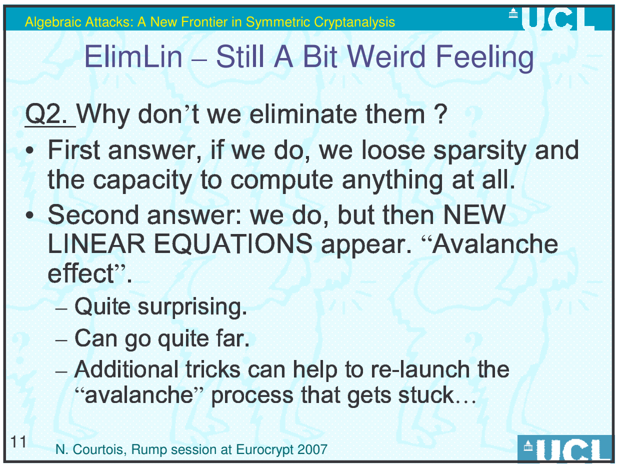
9 N. Courtois, Rump session at Eurocrypt 2007



ElimLin – Something Wrong ?

Q1. Why do we have linear equations in the first place ?

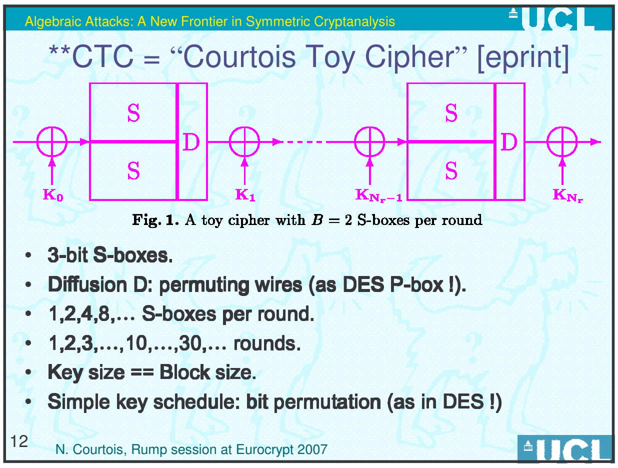
- Stupid in mathematics…
- IMPOSSIBLE TO AVOID in cryptanalysis.
  - E.g. take several KP.
  - Add well-chosen constraints
  - Etc.



ElimLin – Still A Bit Weird Feeling

Q2. Why don’t we eliminate them ?

- First answer, if we do, we loose sparsity and the capacity to compute anything at all.
- Second answer: we do, but then NEW LINEAR EQUATIONS appear. “Avalanche effect”.
  - Quite surprising.
  - Can go quite far.
  - Additional tricks can help to re-launch the “avalanche” process that gets stuck…

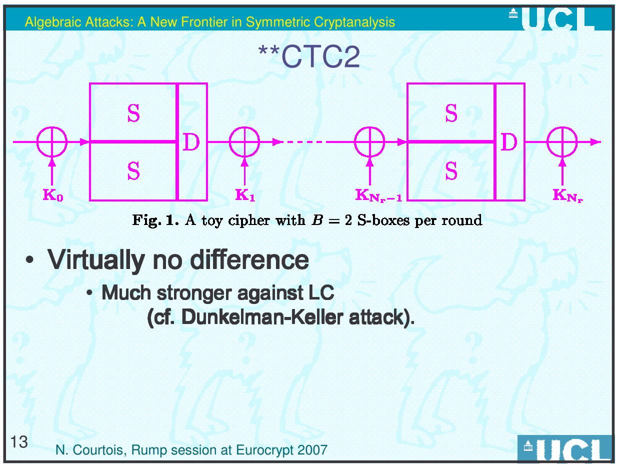


**CTC = “Courtois Toy Cipher” [eprint]

S
S
D
S
S
D
K_0
K_1
K_{N_r-1}
K_{N_r}

Fig. 1. A toy cipher with $B = 2$ S-boxes per round

- **3-bit S-boxes.**
- **Diffusion D: permuting wires (as DES P-box !).**
- **1,2,4,8,… S-boxes per round.**
- **1,2,3,…,10,…,30,… rounds.**
- **Key size == Block size.**
- **Simple key schedule: bit permutation (as in DES !)**

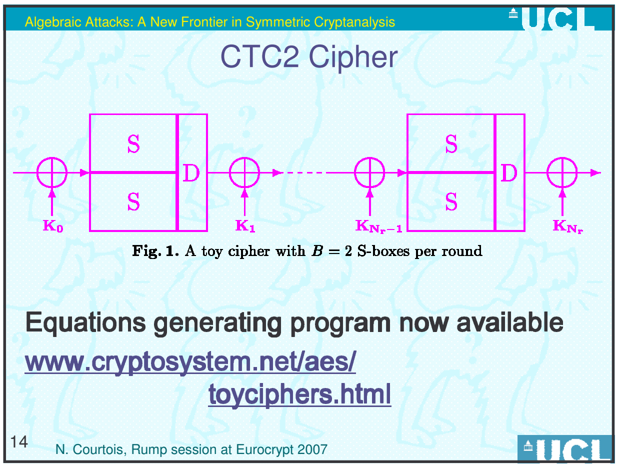


**CTC2

S
S
D
S
S
D
K_0
K_1
K_{N_r-1}
K_{N_r}

Fig. 1. A toy cipher with $B = 2$ S-boxes per round

- Virtually no difference
  - Much stronger against LC (cf. Dunkelman-Keller attack).

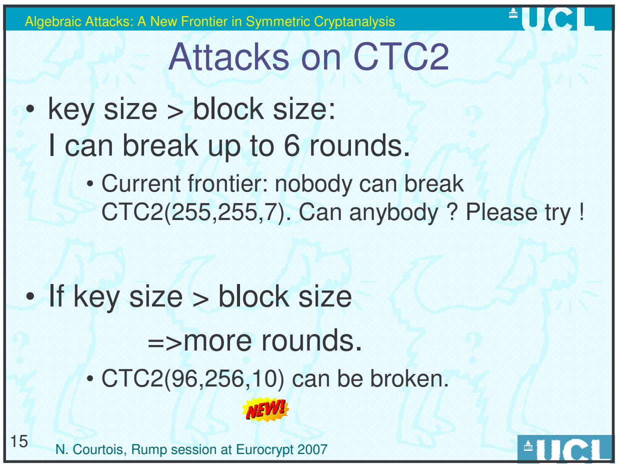


CTC2 Cipher

S
S
D
S
S
D
K_0
K_1
K_{N_r-1}
K_{N_r}

Fig. 1. A toy cipher with $B = 2$ S-boxes per round

Equations generating program now available
www.cryptosystem.net/aes/toyciphers.html

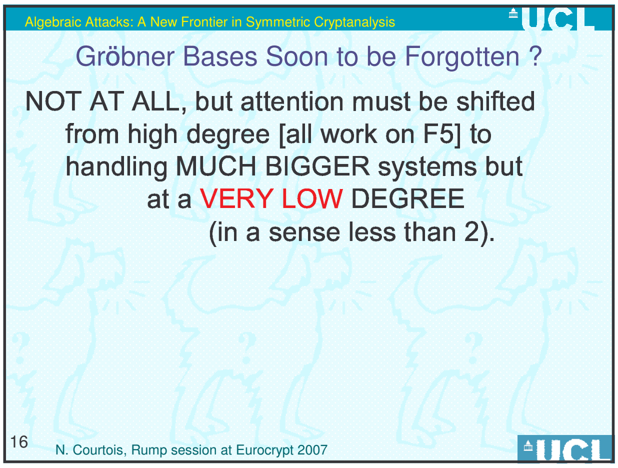


Attacks on CTC2

- key size > block size:
  I can break up to 6 rounds.
  - Current frontier: nobody can break CTC2(255,255,7). Can anybody ? Please try !

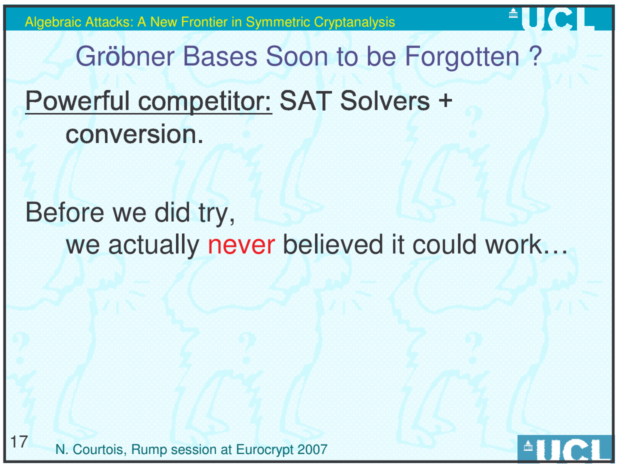
- If key size > block size
  =>more rounds.
  - CTC2(96,256,10) can be broken.

NEW!



Gröbner Bases Soon to be Forgotten ?

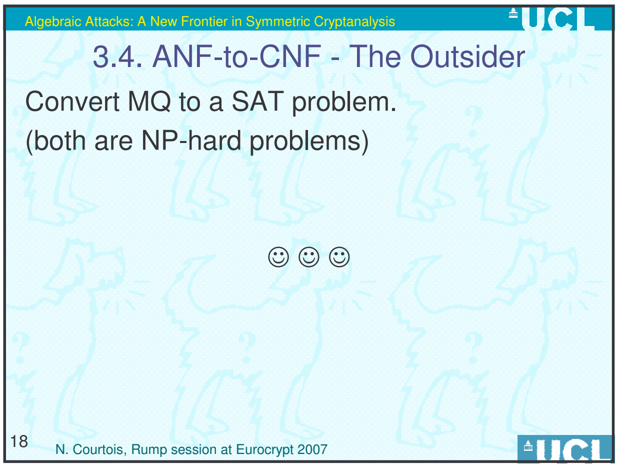
NOT AT ALL, but attention must be shifted from high degree [all work on F5] to handling MUCH BIGGER systems but at a VERY LOW DEGREE (in a sense less than 2).



Gröbner Bases Soon to be Forgotten ?

Powerful competitor: SAT Solvers + conversion.

Before we did try,
we actually never believed it could work…

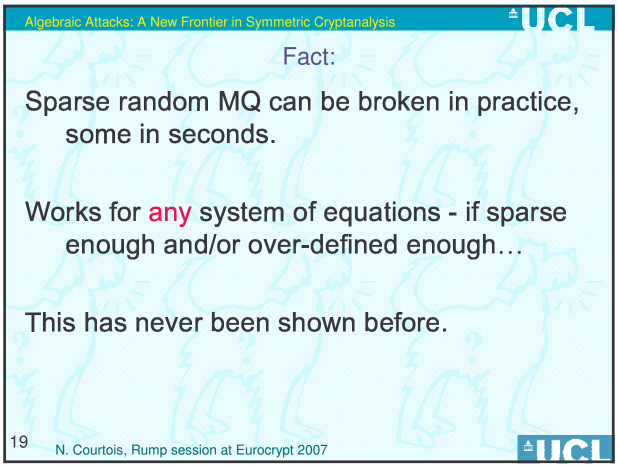


3.4. ANF-to-CNF - The Outsider

Convert MQ to a SAT problem.

(both are NP-hard problems)

☺ ☺ ☺

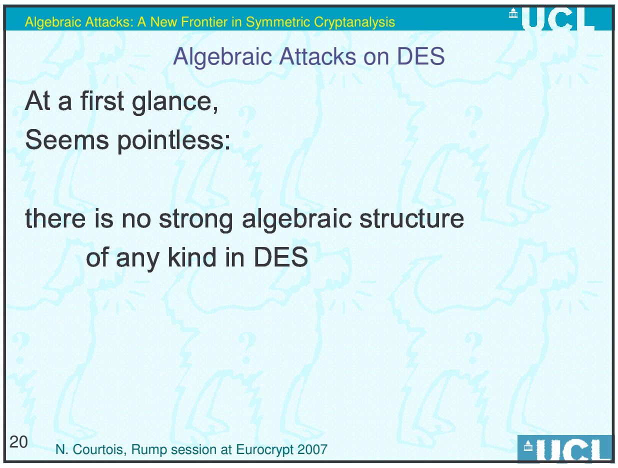


Fact:

Sparse random MQ can be broken in practice, some in seconds.

Works for any system of equations - if sparse enough and/or over-defined enough…

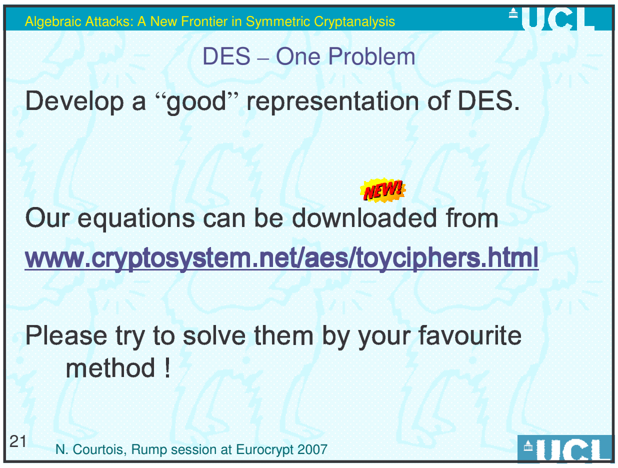
This has never been shown before.



Algebraic Attacks on DES

At a first glance,
Seems pointless:

there is no strong algebraic structure of any kind in DES



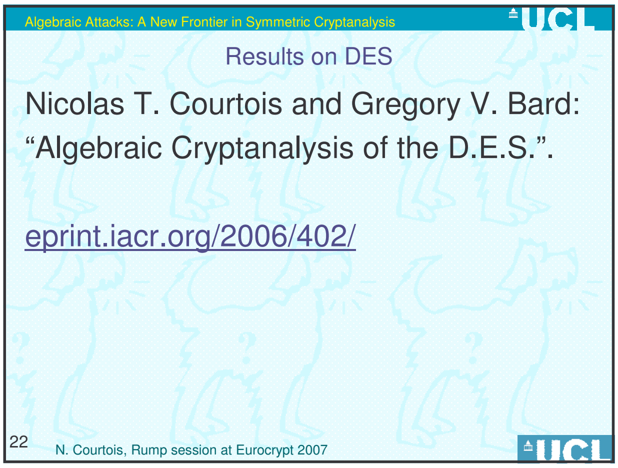
DES – One Problem

Develop a “good” representation of DES.

NEW!

Our equations can be downloaded from
www.cryptosystem.net/aes/toyciphers.html

Please try to solve them by your favourite method !



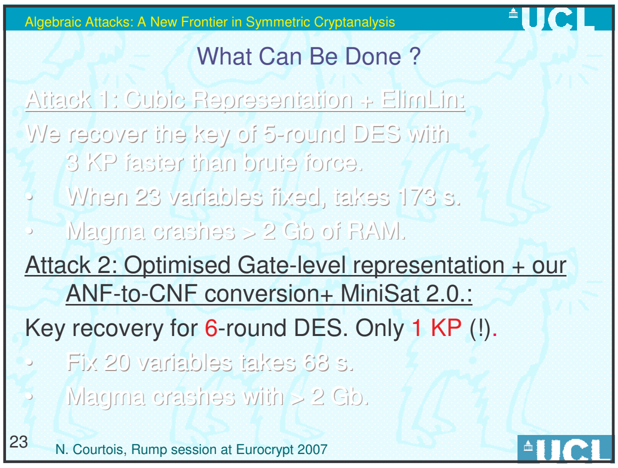
Algebraic Attacks: A New Frontier in Symmetric Cryptanalysis

Results on DES

Nicolas T. Courtois and Gregory V. Bard: “Algebraic Cryptanalysis of the D.E.S.”.

eprint.iacr.org/2006/402/

22 N. Courtois, Rump session at Eurocrypt 2007



Algebraic Attacks: A New Frontier in Symmetric Cryptanalysis

What Can Be Done ?

Attack 1: Cubic Representation + ElimLin:

We recover the key of 5-round DES with 3 KP faster than brute force.

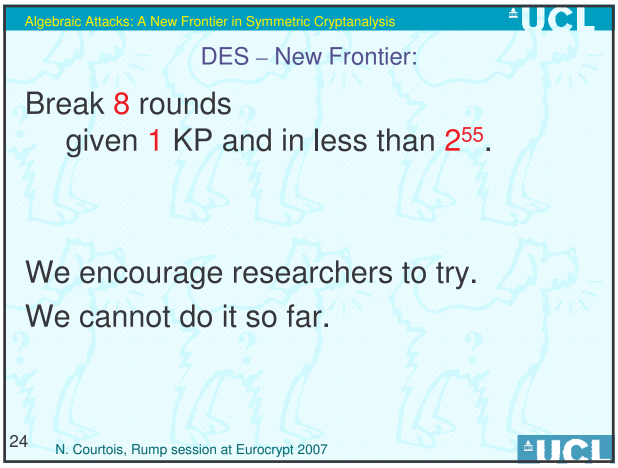
- When 23 variables fixed, takes 173 s.
- Magma crashes > 2 Gb of RAM.

Attack 2: Optimised Gate-level representation + our ANF-to-CNF conversion+ MiniSat 2.0.:

Key recovery for 6-round DES. Only 1 KP (!).

- Fix 20 variables takes 68 s.
- Magma crashes with > 2 Gb.

23 N. Courtois, Rump session at Eurocrypt 2007



Algebraic Attacks: A New Frontier in Symmetric Cryptanalysis

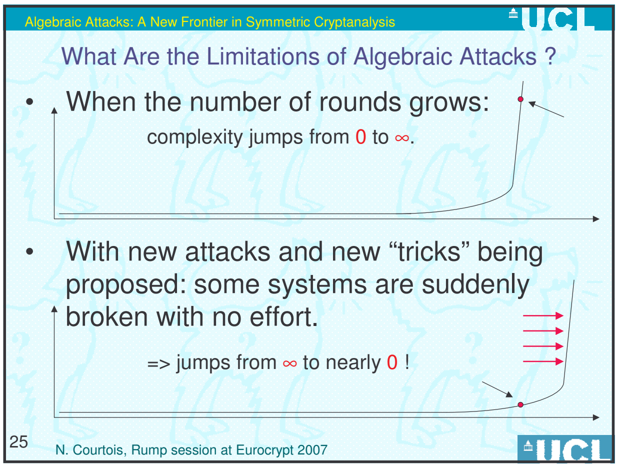
DES – New Frontier:

Break 8 rounds given 1 KP and in less than 2^{55}.

We encourage researchers to try.

We cannot do it so far.

24 N. Courtois, Rump session at Eurocrypt 2007



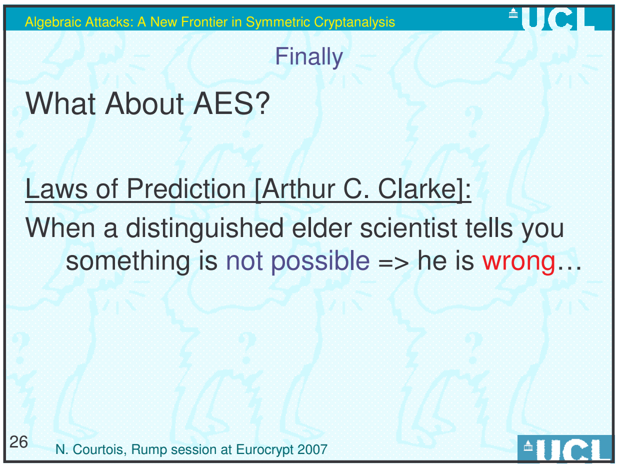
What Are the Limitations of Algebraic Attacks ?

- When the number of rounds grows:

  complexity jumps from 0 to ∞.

- With new attacks and new “tricks” being proposed: some systems are suddenly broken with no effort.

  => jumps from ∞ to nearly 0 !

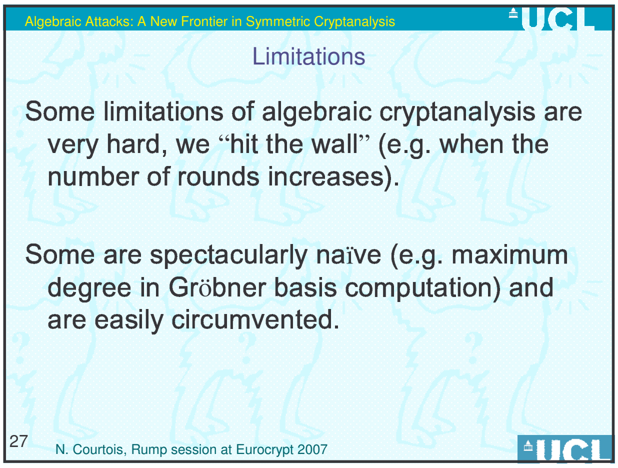


Finally

What About AES?

Laws of Prediction [Arthur C. Clarke]:

When a distinguished elder scientist tells you something is not possible => he is wrong…



Limitations

Some limitations of algebraic cryptanalysis are very hard, we “hit the wall” (e.g. when the number of rounds increases).

Some are spectacularly naïve (e.g. maximum degree in Gröbner basis computation) and are easily circumvented.

Exploring the New Frontier

We need yet to discover what is hard and what is not.

=>

I propose a new tool to help researchers making honest and responsible statements:

=> Bets on the future attacks. NEW!

New Tool - Bets

For the first time in history, it is possible to bet on cryptographic algorithms with real money.

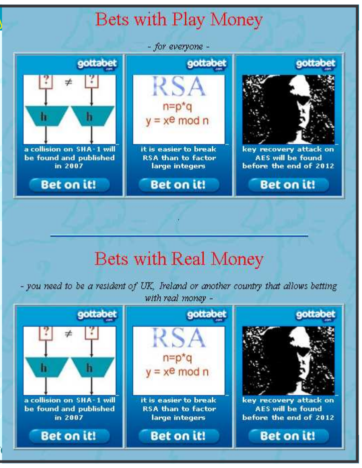
This has never been possible before.

See www.cryptobet.com. NEW!

Purpose: have fun and show the advancement of cryptographic research. It is a game.

Current Bets:

I encourage people to propose new bets related to their own research.



Bets with Play Money

- for everyone -

a collision on SHA-1 will be found and published in 2007

it is easier to break RSA than to factor large integers

key recovery attack on AES will be found before the end of 2012

Bets with Real Money

- you need to be a resident of UK, Ireland or another country that allows betting with real money -

a collision on SHA-1 will be found and published in 2007

it is easier to break RSA than to factor large integers

key recovery attack on AES will be found before the end of 2012