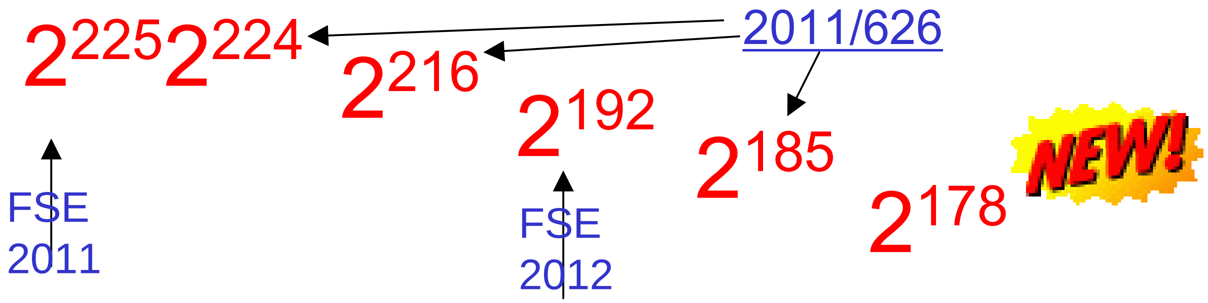


2^{225} 2^{224} 2^{216} 2^{192} 2^{185} 2^{178} NEW!

2011/626

FSE 2011

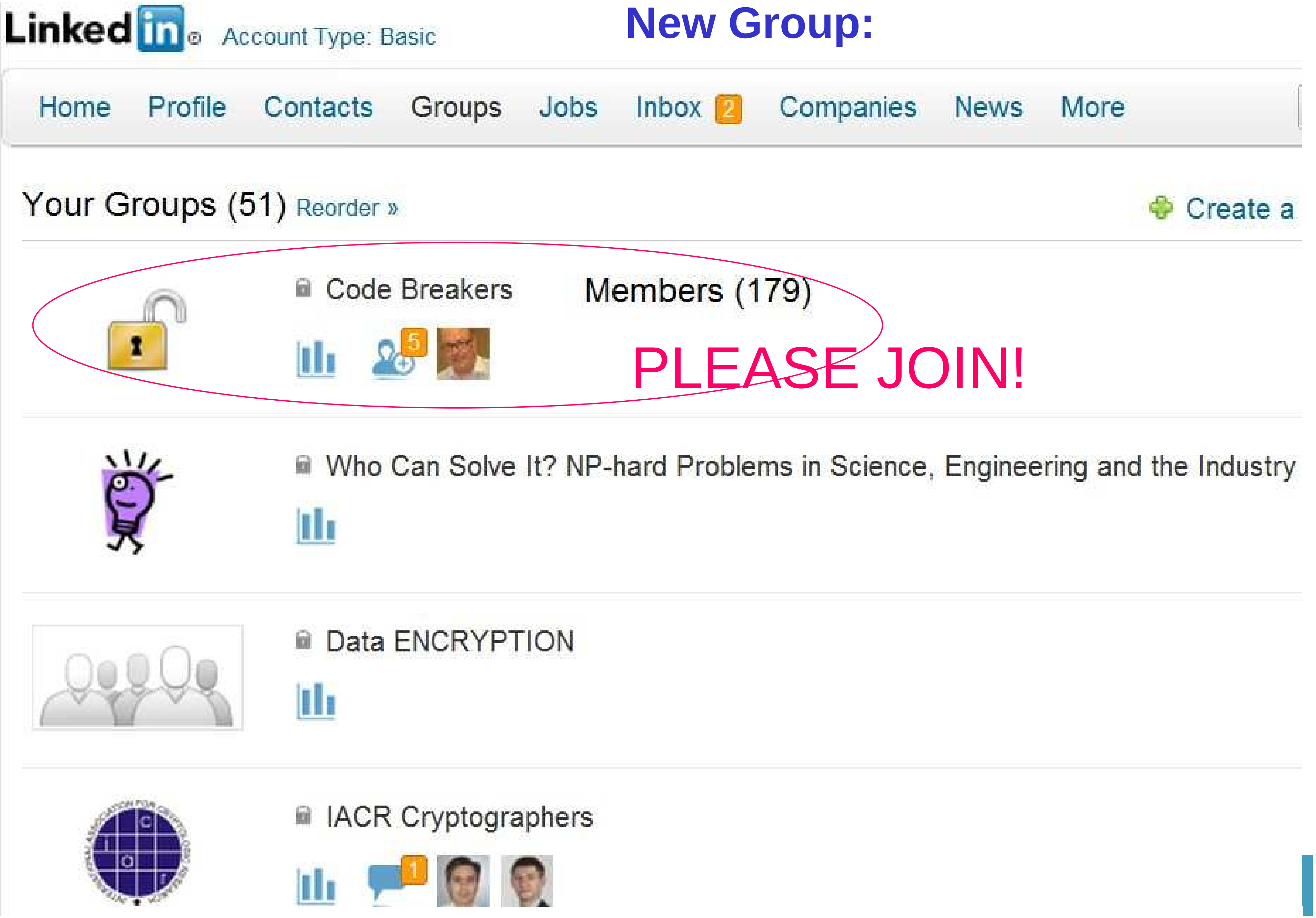
FSE 2012

Faster Attacks on Full GOST

Nicolas T. Courtois

University College London, UK

New Group:



Linked in Account Type: Basic

Your Groups (51) Reorder »

Code Breakers Members (179)

PLEASE JOIN!

Who Can Solve It? NP-hard Problems in Science, Engineering and the Industry

Data ENCRYPTION

IACR Cryptographers

Russian Subtitles On:

code breakers ==

взломщики кодов

GOST Cipher

трудновскрываемый шифр

BEWARE

I’m going to cheat you
and totally ignore
the large data complexity
of many attacks…

⇒ just compare the running time

GOST Block Cipher

It is NOT correct to compare GOST to DES.

- 256 bits key = a military level of security
- a former "Top Secret" government algorithm used by major banks etc…
  - not a commercial algorithm like DES…
  - DES was "breakable" from day 1
    - due to reduced key space = 56 bits
- DES could be used ONLY for unclassified documents. In contrast:
- GOST "does not place any limitations on the secrecy level of the protected information"
  - cf. preface to English translation of GOST, by Aleks. Malchik and Whit Diffie

GOST in ISO

- In 2010 GOST was also submitted to ISO to become an international standard.
- In the mean time GOST was broken…
  - plethora of new attacks…

Black-Box Algebraic Complexity Reduction

Black Box Complexity Reduction Paradigm [Courtois 2011]

Black-box
high-level
guess and determine methods
which transform
an attack on 32 rounds of GOST
into an attack on e.g. 8 rounds of GOST
with much less data.

Reductions

- Given 2^X KP for the full 32-round GOST.
- Obtain Y KP for 8 rounds of GOST.
- This valid with probability 2^{-Z}.
- For a proportion 2^{-T} of GOST keys.

Two examples were given on Monday.

As many 18 distinct reductions of this type with a large variety of 2^X,Y, 2^{-Z}, 2^{-T} can be found at

eprint/2011/626

Black-Box Complexity Reduction - Already Known?

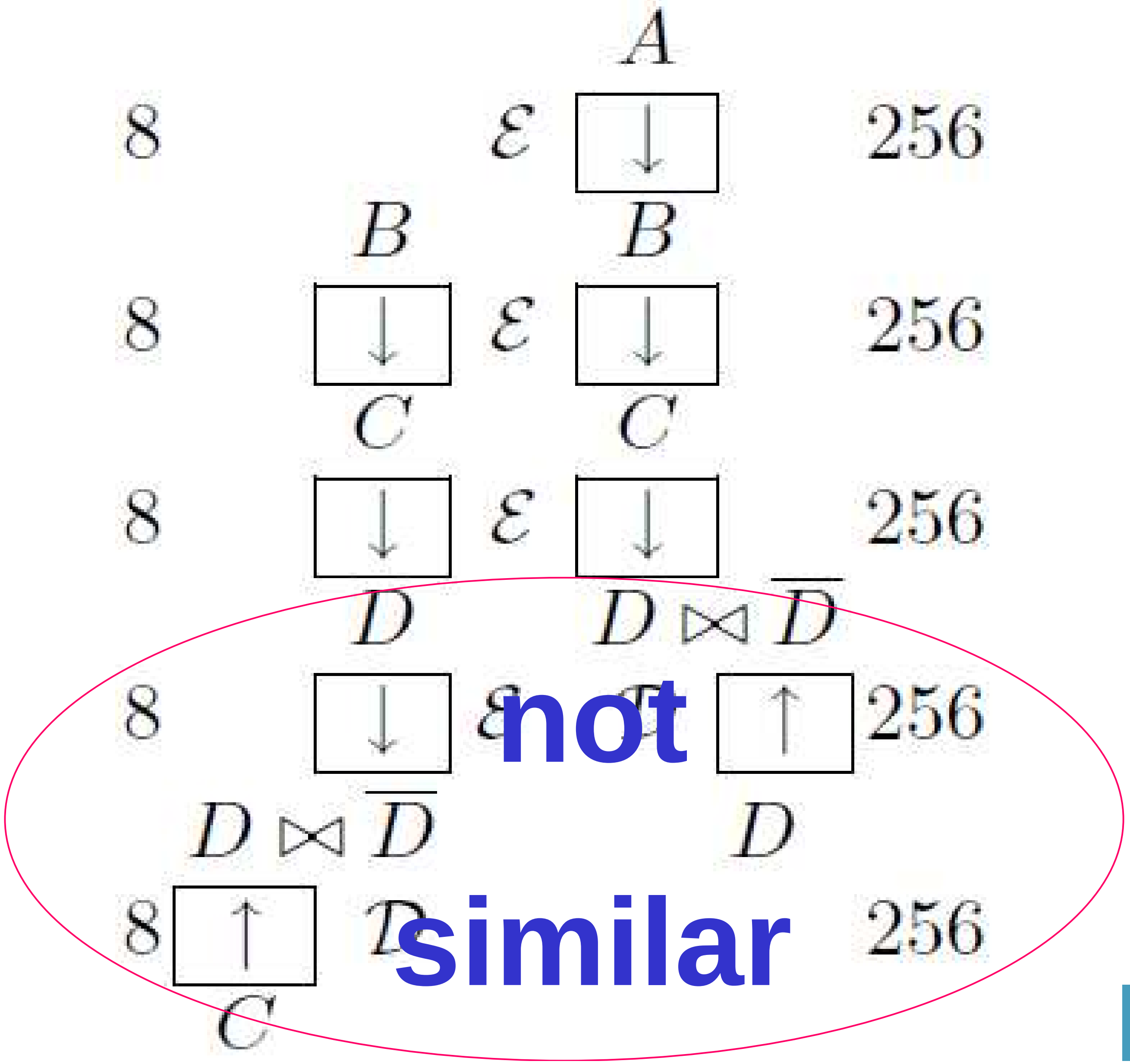
Slide / Fixed Point / Cycling / Guess-Det. / Involution / Etc..

WHAT'S NEW?

- There are now many completely new attacks which are exactly none of the above [though similar or related].
- Many of these attacks were <u>never studied</u> because they generate only a few known plaintexts, and only in the last 5 years it became possible to design an appropriate last step for these attacks which is a low-data complexity key recovery e.g.
  - software algebraic attack
  - MITM attack, also gets highly non-trivial as seen on Monday…

One Example of Black Box Reduction

Appears in Cryptologia, Issue 1, 2012



not

similar

Which Attacks on GOST Are Now The Fastest?

A Very Weird Attack

In eprint/2011/626, Fact 23, page 41.

With probability 2^{-32} over the 256-bit keys, they key can be recovered in time of 2^{154}.

Observe that

$2^{32} \times 2^{154} =$ ONLY 2^{186}

$< 2^{192}$ [FSE 2012]

Compare:

Courtois Attacks 2011/626

2^{216} 2^{216}

Fact 12 Fact 13

63 % another 63 %

2^{154}

Fact 23

2^{-32}

2^{121}

Fact 27

2^{-64}

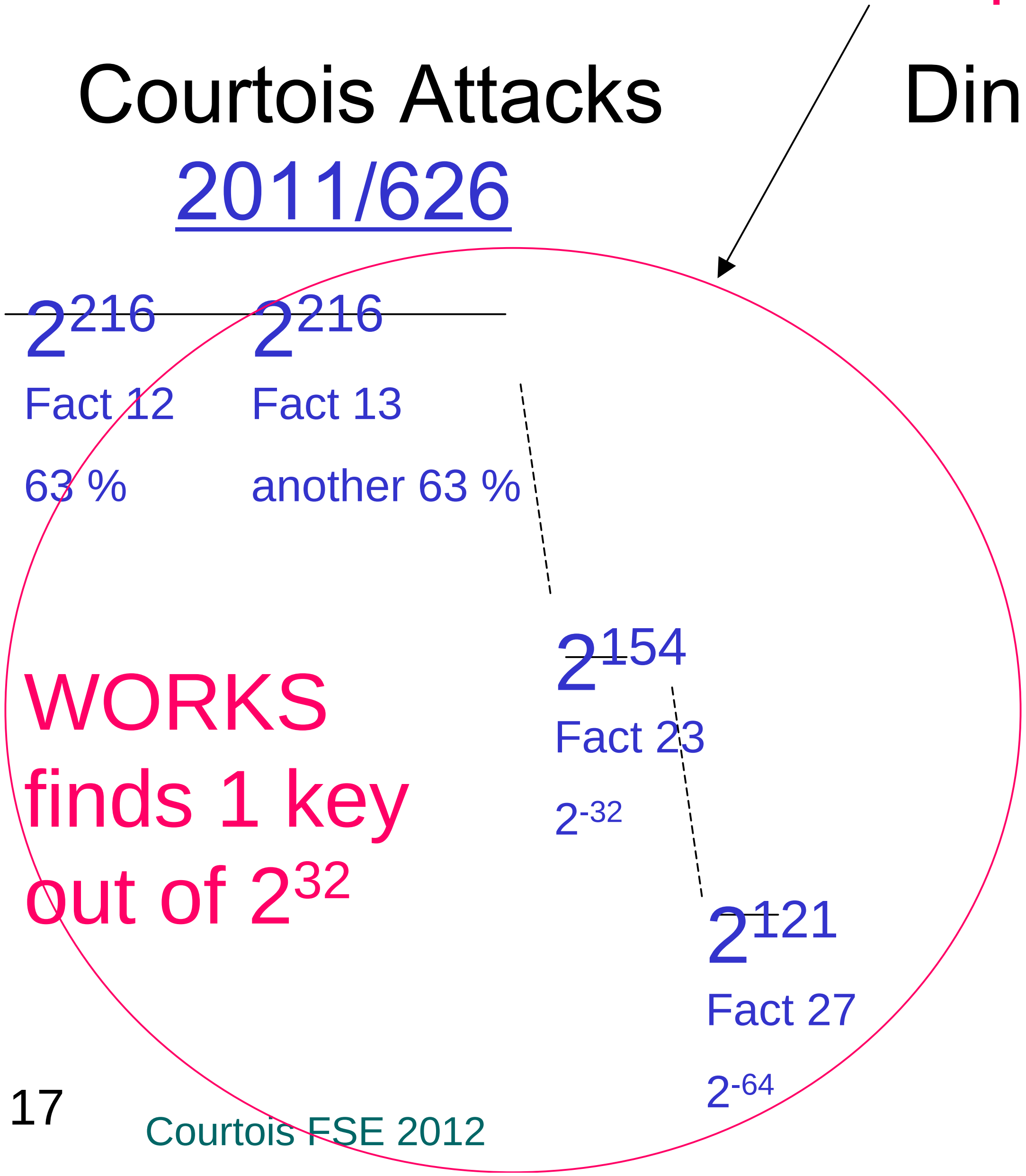
Dinur-Dunkelman-Shamir FSE 2012

2^{192}

what if we CAN do 2^{186} computations but not more

Courtois Attacks 2011/626

Dinur-Dunkelman-Shamir FSE 2012



2^{216} 2^{216}

Fact 12 Fact 13

63 % another 63 %

2^{154}

Fact 23

2^{-32}

2^{121}

Fact 27

2^{-64}

WORKS

finds 1 key

out of 2^{32}

2^{192}

FAILS☹

Conclusion:

Single Key Attacks

do NOT capture

realistic attacks
with random and
uniformly distributed keys

Last But Not Least

Latest Attack on GOST [March 2012]

Most Recent Attack

NEW!

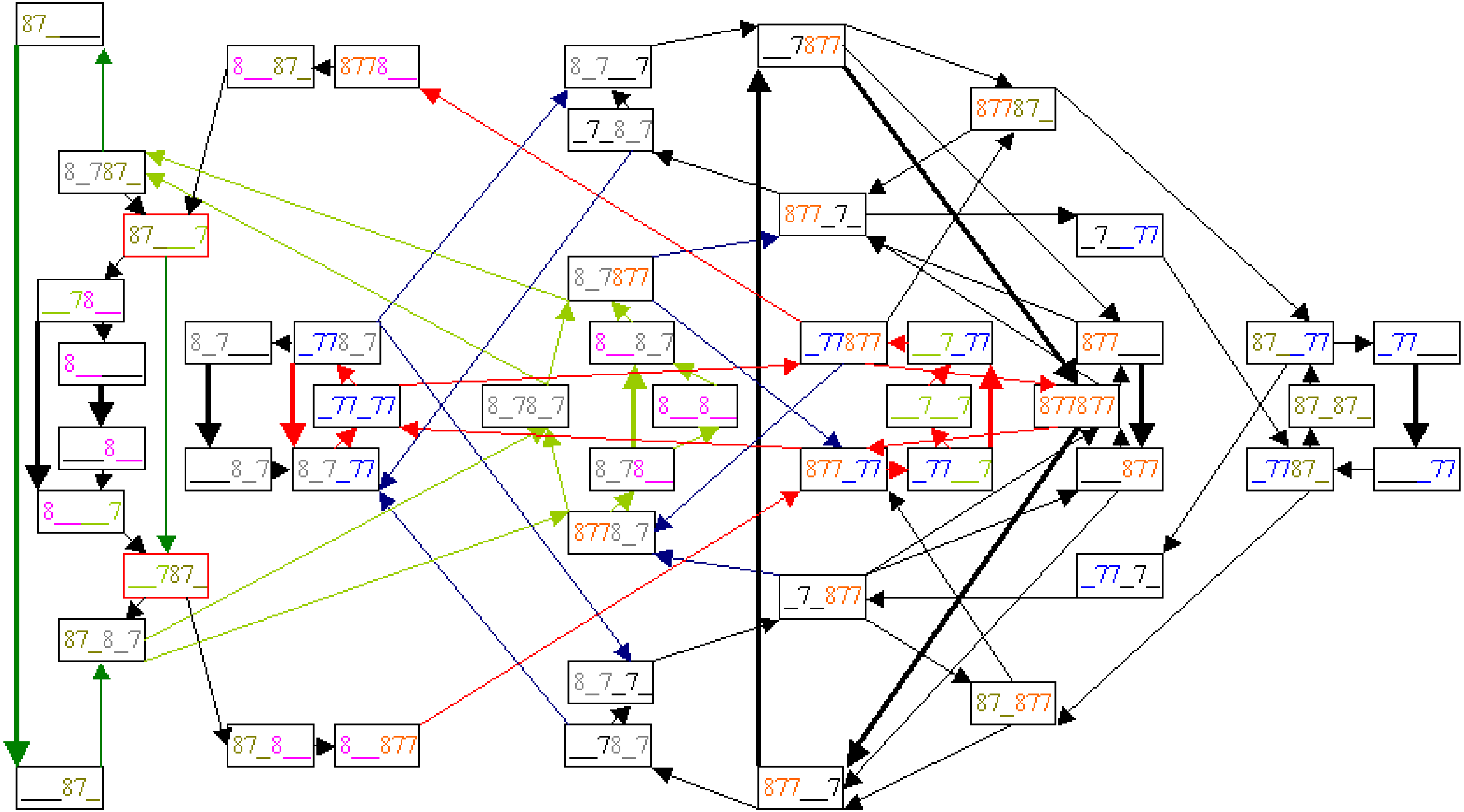
- a true single key attack.
- based on sets of differentials.
- T = 2^{178}, better than any previous.
- submitted to eprint last week.

How To Find Such An Attack

Best differential property
we ever found was found BY HAND.

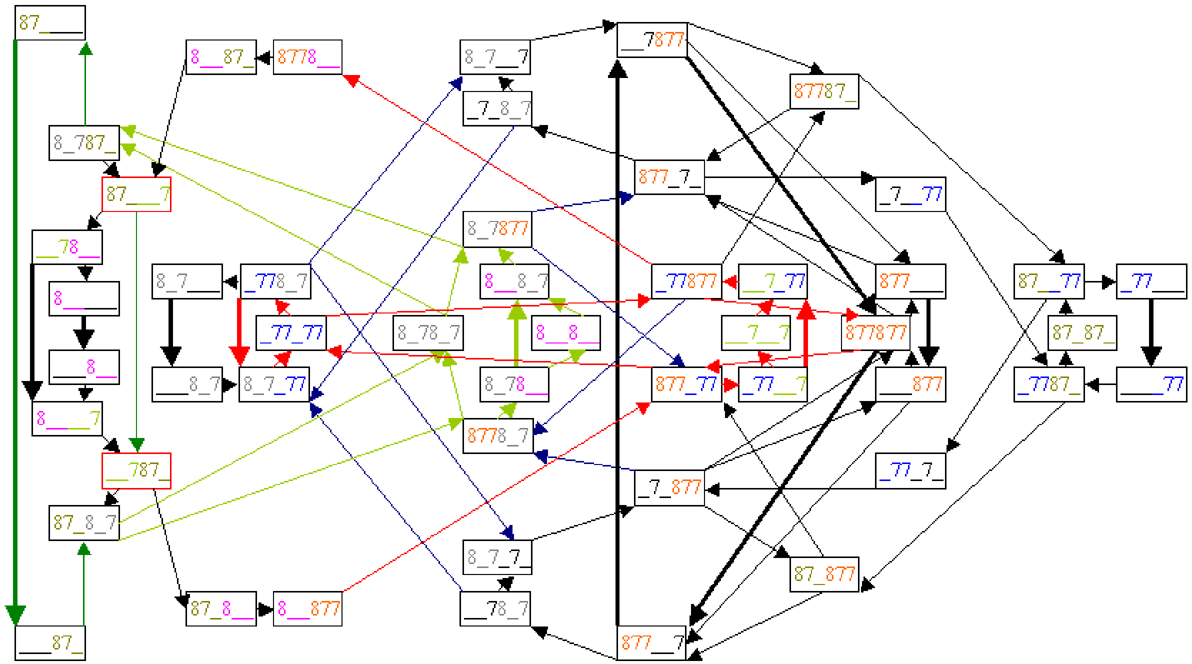
Is systematic approach possible?

Our Attack = Graph Walks With Costs



Remark:

- the structure of this graph does NOT depend on the S-boxes
- only costs (probabilities) depend on the S-boxes


87___
8__87_
8778__
8_7__7
_7_8_7
__7877
87787_
8_787_
87___7
877_7_
_7__77
8_7877
__78__
8_7___
_778_7
8__8_7
_77877
__7_77
877___
87__77
_77___
8____
_77_77
8_78_7
8__8__
__7__7
877877
87_87_
___8__
___8_7
8_7_77
8_78__
877_77
_77__7
___877
_7787_
____77
8___7
8778_7
__787_
_77_7_
87_8_7
_7_877
8_7_7_
87_877
87_8__
8__877
__78_7
877__7
___87_