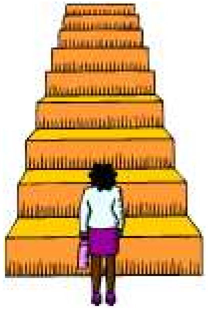
Self-Similarity Composition of Permutations

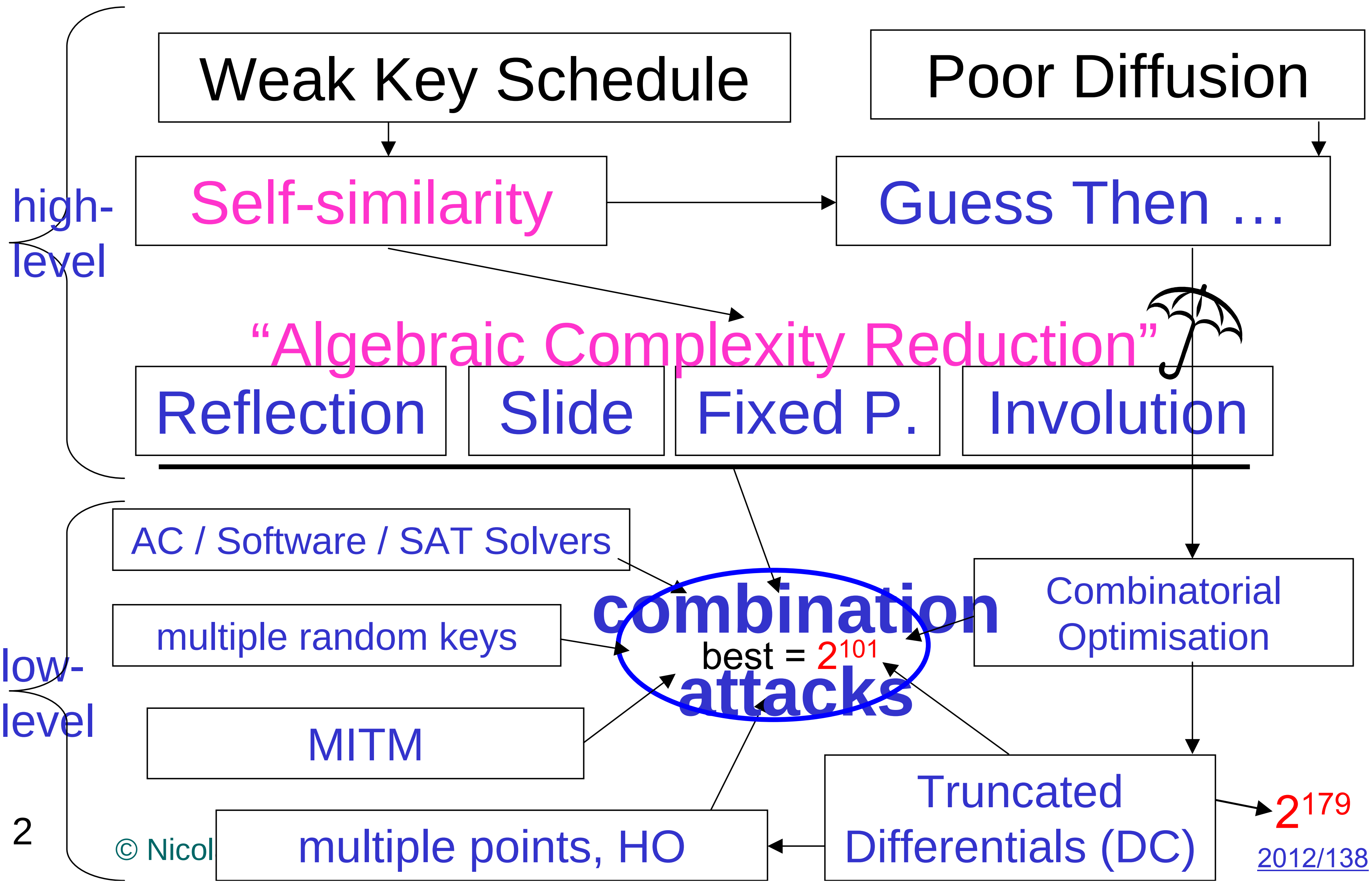


Nicolas T. Courtois

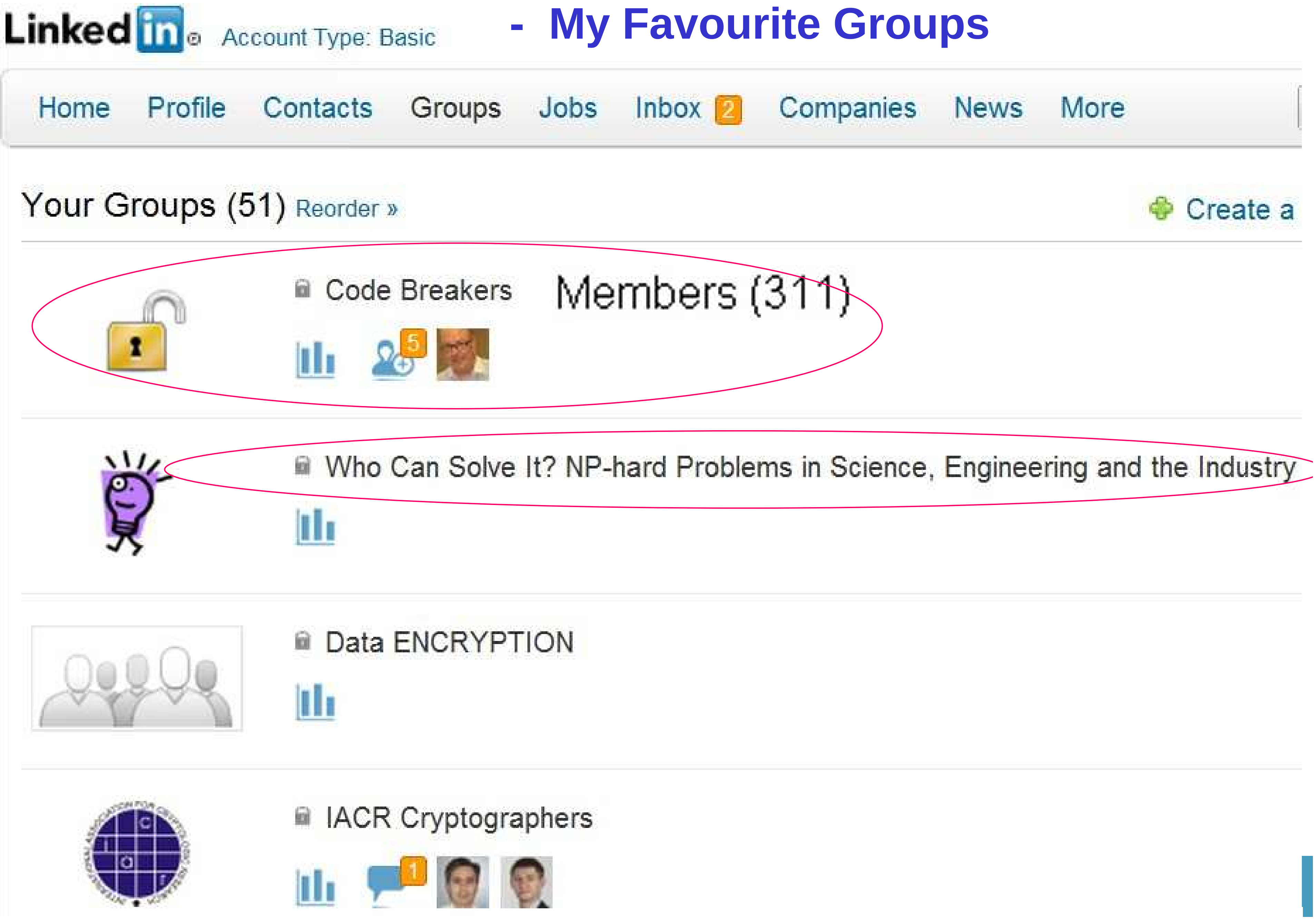
University College London, UK

What's Wrong? >50 distinct attacks… Best = 2^{101}

cf. 2011/626



- My Favourite Groups



Russian Subtitles On:

code breakers ==

взломщики кодов

Cryptanalysis

from Greek

- kryptós, "hidden“
- analýein, "to untie“

Term coined in 1920

by William F. Friedman.

- Born in Moldavia, emigrated to US in 1892.
- Chief cryptologist at National Security Agency in the 50s.

2. Modern 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]

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) ?

LOW DATA CRYPTANALYSIS NEW!

Two Worlds:

- **The “approximation” cryptanalysis:**
  - Linear, differential, approximation, attacks etc..
  - based on probabilistic characteristics
    - true with some probability.
  - consequently, <u>the security will grow exponentially</u> with the number of rounds, and <u>so does the number of required plaintexts</u> in the attacks
    - main limitation in practice.
- **The “exact algebraic” approach:**
  - Write equations to solve, true with probability 1.

    => Low data complexity

What Can be Done ?

Algebraic Cryptanalysis:

- Very special ciphers: 1 M rounds [Courtois'AES4].
- General ciphers:
  SMALL number of rounds, 4,5,6 rounds.
  - If key size > block size – more rounds.
  - CTC2(96,256,10) can be broken.

Def: "I / O Degree" = "Graph AI"

Consider function $f : GF(2)^n \rightarrow GF(2)^m$, $f(x) = y$, with $x = (x_0, \ldots, x_{n-1})$, $y = (y_0, \ldots, y_{m-1})$.

Definition [The I/O degree] The I/O degree of f is the smallest degree of the algebraic relation

$$g(x_0, \ldots, x_{n-1}; y_0, \ldots, y_{m-1}) = 0$$

that holds with certainty for every couple (x, y) such that $y = f(x)$.

A "good" cipher should use at least some components with high I/O degree.

Early Work on Algebraic Attacks on Ciphers

- [2002] XSL paper:

2 “crazy” conjectures:

very small S-boxes

– I/O Degree Hypothesis (**IOH**): all ciphers with low I/O degree and lots of I/O relations may be broken ?
– The Very Sparse Hypothesis (**VSH**): ciphers with very low gate count broken ?

Algebraic Attacks on Block Ciphers

1. Write +
2. Solve [key recovery].

Conversion

Algebraic equations (ANF) => SAT Problem

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”.

Ready Software

Several ready programs to perform this conversion are made available on this web page:

www.cryptosystem.net/aes/tools.html

SAT Solvers in the Cloud

UCL spin-off company

solving SAT problems on demand…

commercial but also for free…

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”.

Ready Software for Windows

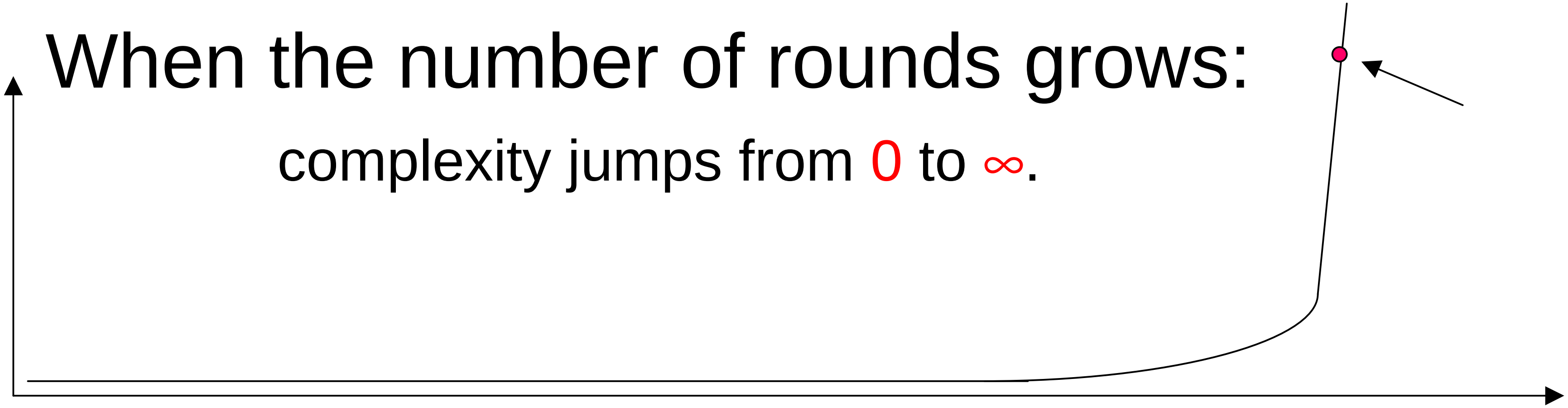
Ready programs:

www.cryptosystem.net/aes/tools.html

What Are the Limitations of Algebraic Attacks ?

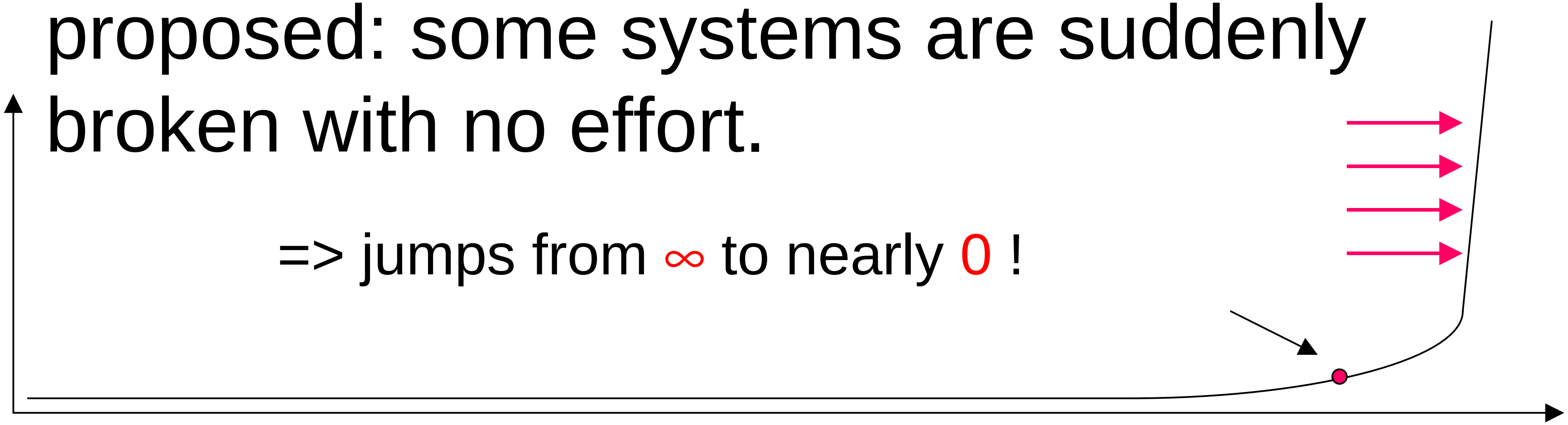
- When the number of rounds grows:

  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 !



DES

At a first glance,

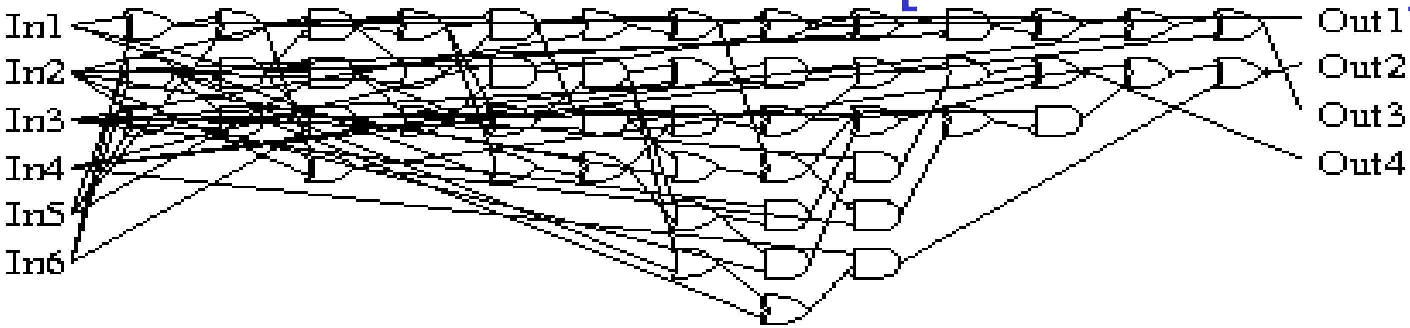
DES seems to be a very poor target:

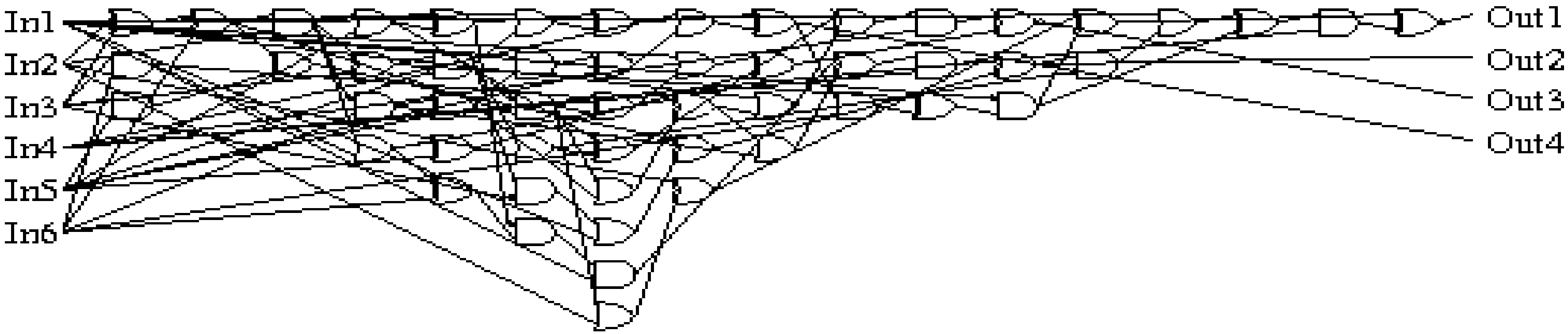
there is (apparently)

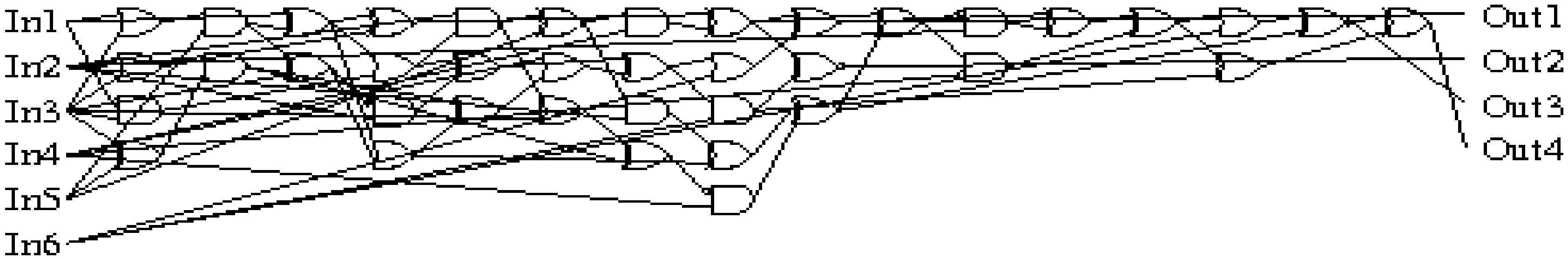
no strong algebraic structure

of any kind in DES

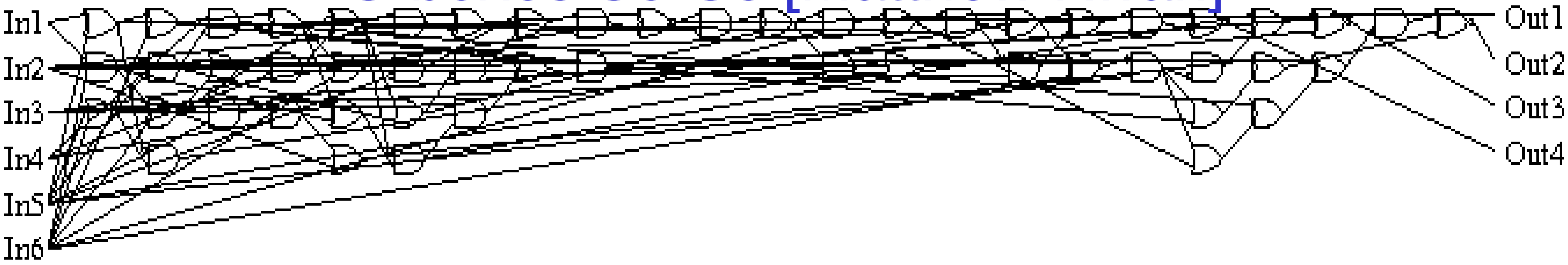
S-boxes S1-S4 [Matthew Kwan]

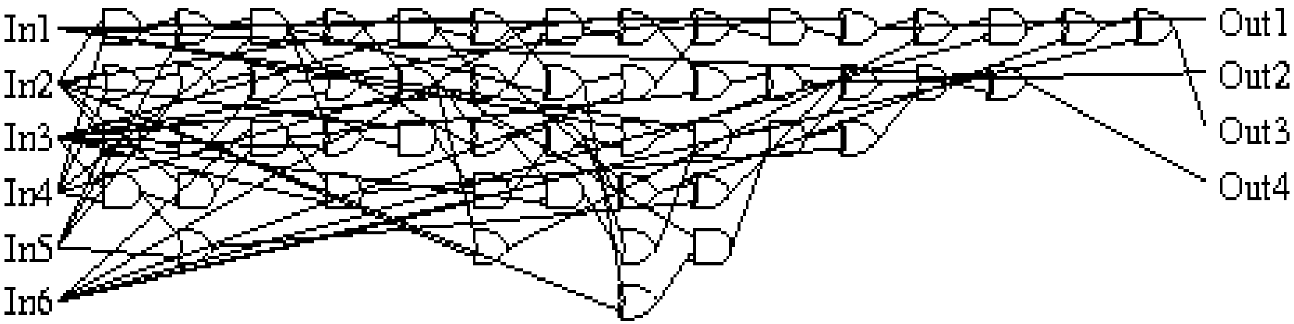






S-boxes S5-S8 [Matthew Kwan]





I / O Degree

Consider function $f : GF(2)^n \to GF(2)^m$,
$f(x) = y$, with $x = (x_0, \ldots, x_{n-1})$, $y = (y_0, \ldots, y_{m-1})$.

Definition [The I/O degree] The I/O degree of f is the smallest degree of the algebraic relation

$$g(x_0, \ldots, x_{n-1}; y_0, \ldots, y_{m-1}) = 0$$

that holds with certainty for every couple (x, y) such that $y = f(x)$.

A "good" cipher should use at least some components with high I/O degree.

Results on DES

Nicolas T. Courtois and Gregory V. Bard:

Algebraic Cryptanalysis of the D.E.S.

In IMA conference 2007, pp. 152-169, LNCS 4887, Springer.

See also:

eprint.iacr.org/2006/402/

What Can Be Done ?

Idea 1 (Cubic IOH) + 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.

Idea 2 (VSH^{40}) + ANF-to-CNF + MiniSat 2.0.:

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

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

And GOST?

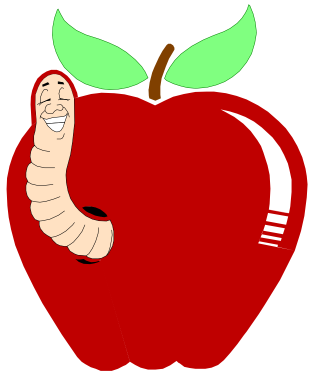
Essentially the same software methods…

well, actually with a lot of non-trivial super-compact representation and circuit optimisation work, cf. our paper at http://2012.sharcs.org/record.pdf.

… allow also to break up to 8 rounds of GOST…

Can we hope to break 32 rounds?

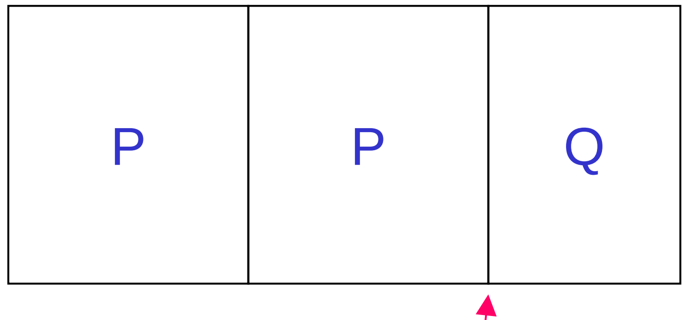
4. Self Similarity



or What's Wrong With Some Ciphers

KEY IDEA

REDUCE the complexity.
For example:
REDUCE the number of rounds.



How? Use self-similarity and high-level structure.

Magic process which allows the attacker to guess/determine values INSIDE the cipher.

We now call it Algebraic Complexity Reduction [Courtois 2011]

4.3. Self-Similarity and KeeLoq

KeeLoq

- Designed in the 80's by Willem Smit.
- In 1995 sold to Microchip Inc for more than 10 Million of US$.

How Secure is KeeLoq

According to Microchip, KeeLoq should have ``a level of security comparable to DES''. Yet faster.

Miserably bad cipher, main reason:

its periodic structure: cannot be defended. The complexity of most attacks on KeeLoq does NOT depend on the number of rounds of KeeLoq.

Notation

f_k() – 64 rounds of KeeLoq

g_k() – 16 rounds of KeeLoq, prefix of f_k().

We have: $E\_k = g\_k \circ f^8\_k$.

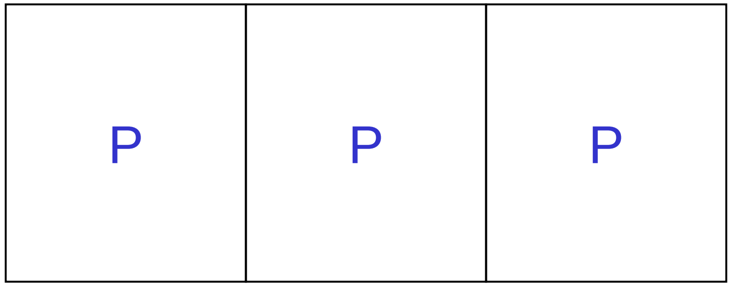
$528 = 16+8*64$ rounds.

4.4. Sliding Properties of KeeLoq

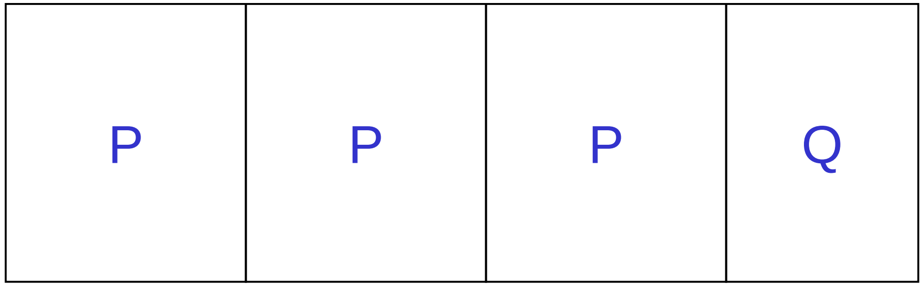
[and one simple attack from FSE 2008]

Sliding Attacks – 2 Cases

- **Complete periodicity [classical].**



- **Incomplete periodicity [new] – harder.**

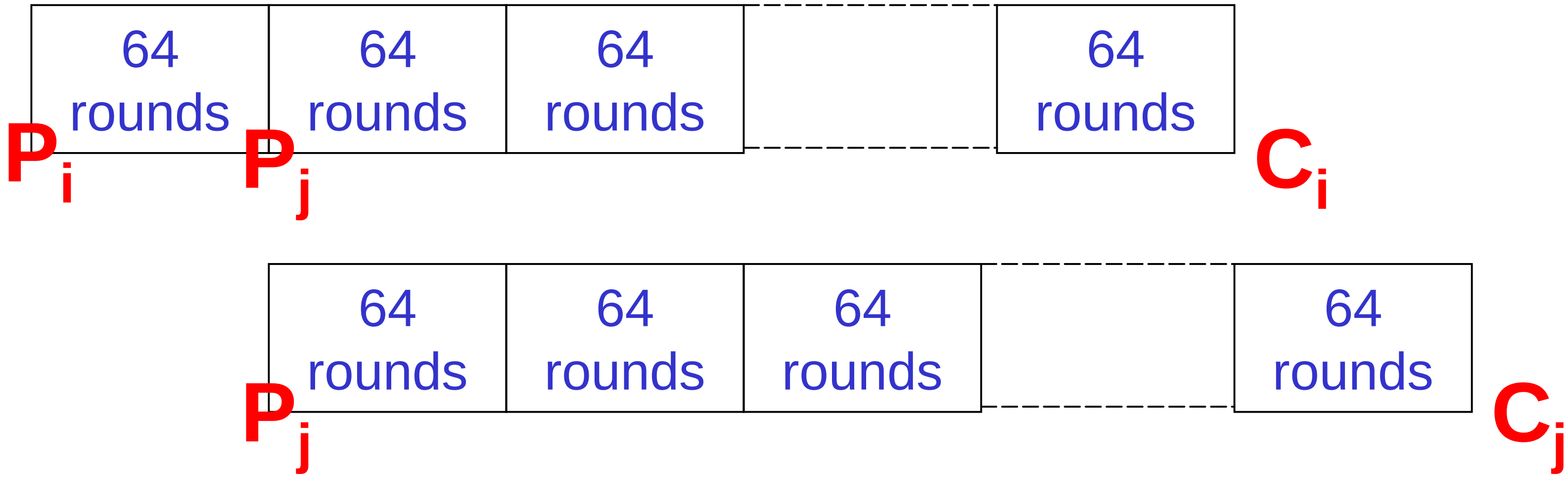


  - **KeeLoq: Q is a functional prefix of P. Helps a lot.**

Sliding Attacks

Classical Sliding Attack [Grossman-Tuckerman 1977]:

- Take $2^{n/2}$ known plaintexts (here n=32, easy !)
- We have a "slid pair" (P_i,P_j) s.t.



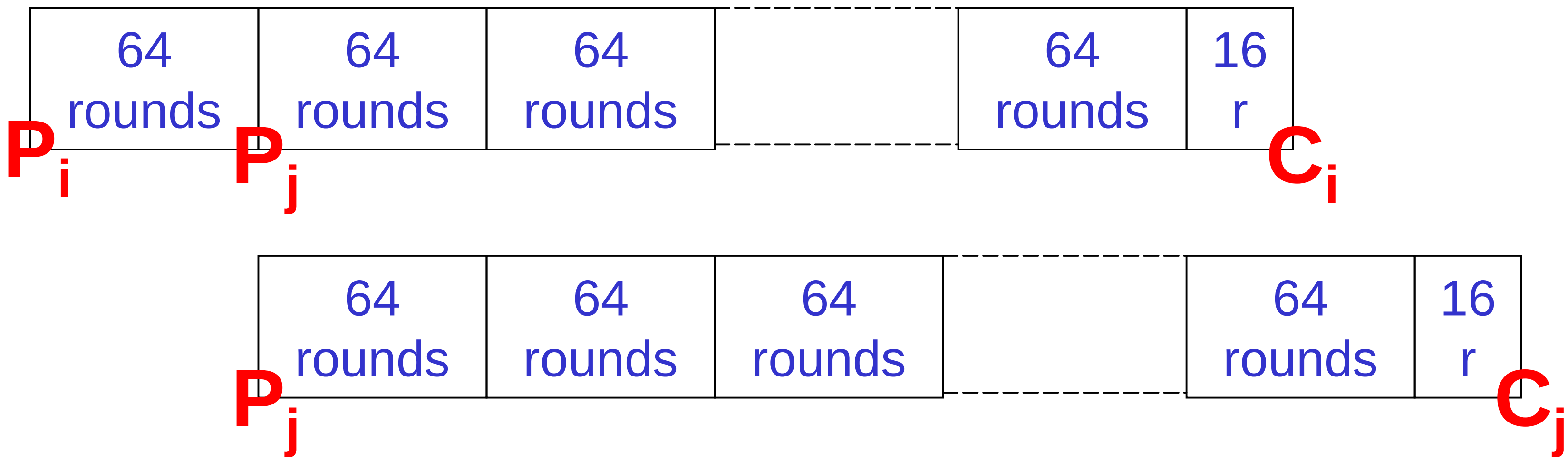
Gives an unlimited number of other sliding pairs !!!

very large **"Amplification"**

KeeLoq and Sliding

Apply Classical Sliding? Attack 1.

- Take $2^{n/2}$ known plaintexts (here n=32, easy !)
- We have a “slid pair” (P_i,P_j) s.t.

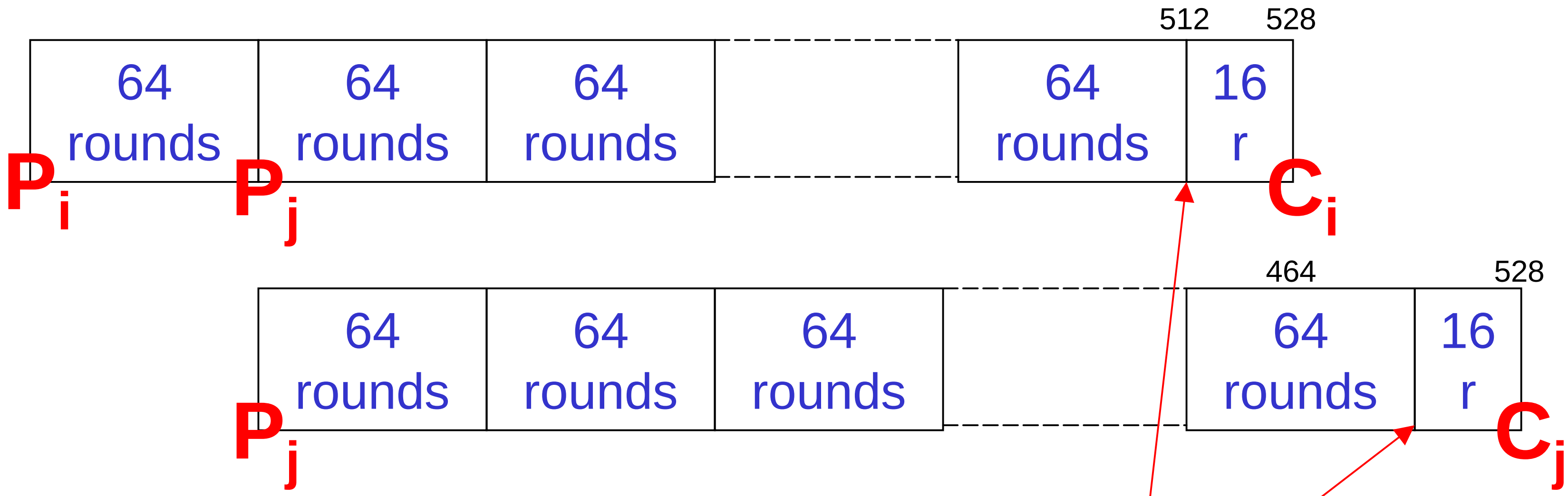


Classical sliding fails – because of the “odd” 16 rounds:

Classical Sliding –Not Easy

Classical Sliding Attack [Grossman-Tuckerman 1977]:

- Take $2^{n/2}$ known plaintexts (here n=32, easy !)
- We have a “slid pair” (P_i,P_j).

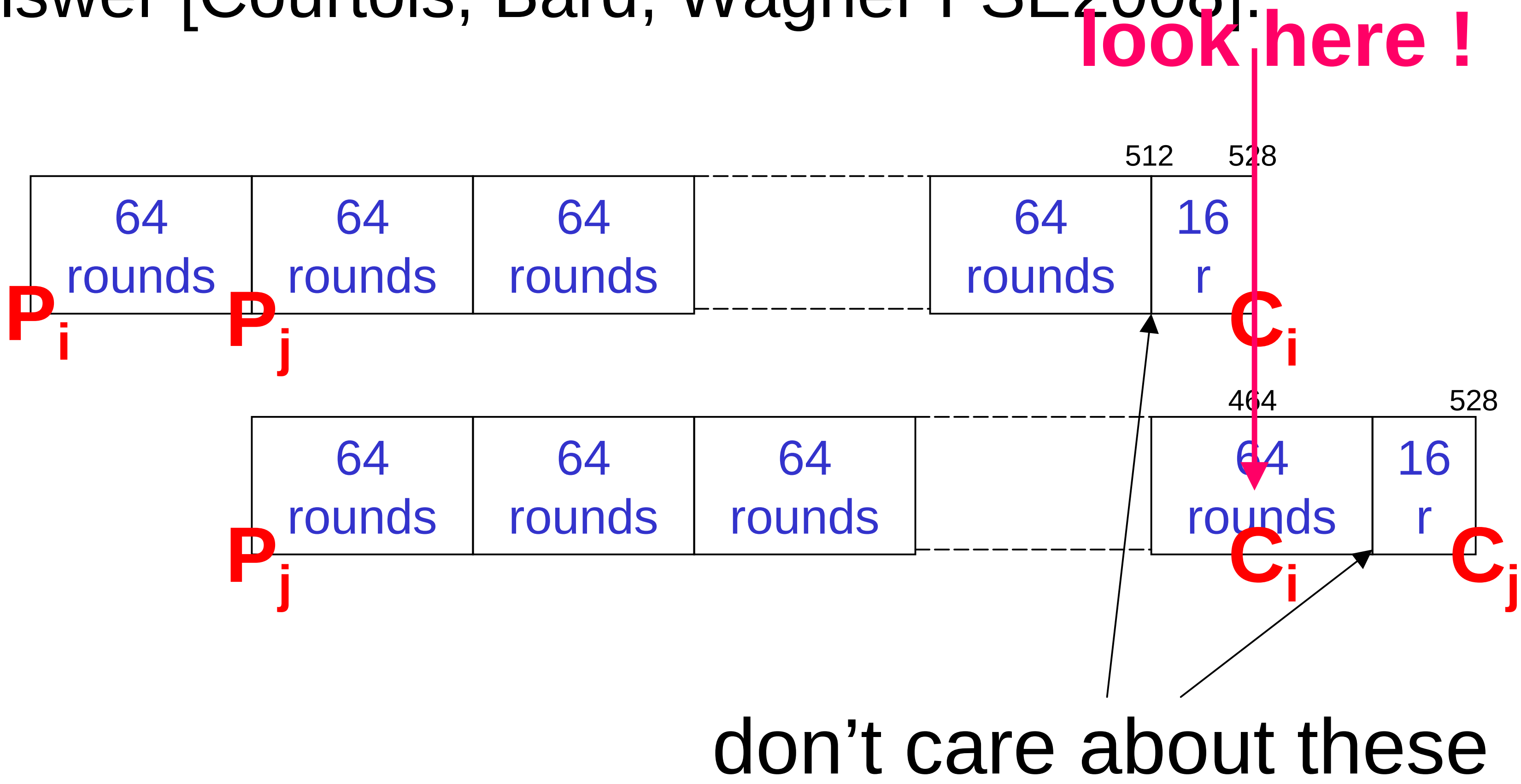


HARD - Problem:

What’s the values here ?

Algebraic Sliding

Answer [Courtois, Bard, Wagner FSE2008]:



Algebraic Attack [FSE 2008]

We are able to use C_i,C_j directly !

Write and merge 2 systems of equations:

System of Equations

64-bit key. Two pairs on 32 bits.
Just enough information.

Attack:

- Write an MQ system.
  - Gröbner Bases methods – miserably fail.
- Convert to a SAT problem
  - [Cf. Courtois, Bard, Jefferson, eprint/2007/024/].
- Solve it.
  - Takes 2.3 seconds on a PC with MiniSat 2.0.

Attack Summary:

Given about 2^{16} KP.

We try all 2^{32} pairs (P_i,P_j).

- If OK, it takes 2.3 seconds to find the 64-bit key.
- If no result - early abort.

Total attack complexity about 2^{64} CPU clocks which is about 2^{53} KeeLoq encryptions.

4.6. Snow 2.0. Cipher

ISO

- Less than 10 crypto algorithms were ever standardized by ISO. E.g. AES.
- All in ISO 18033.
  - Snow 2.0. is an international standard for stream cipher encryption.
  - In 2010 the Russian National Standard GOST was also submitted to ISO 18033 to become an international standard.

I / O Degree (a.k.a. [Graph] Alg. Immunity)

Consider function $f : GF(2)^n \rightarrow GF(2)^m$, $f(x) = y$, with $x = (x_0, \ldots, x_{n-1})$, $y = (y_0, \ldots, y_{m-1})$.

Definition [The I/O degree] The I/O degree of f is the smallest degree of the algebraic relation

$$g(x_0, \ldots, x_{n-1}; y_0, \ldots, y_{m-1}) = 0$$

that holds with certainty for every couple (x, y) such that $y = f(x)$.

Modular Addition

+ modulo 2^{32}

in several ciphers: GOST, SNOW 2.0.

$$(x, y) \mapsto z = x \boxplus y \mod 2^n$$

Theorem 6.1.1. The Multiplicative Complexity (MC) of the addition modulo 2^n is exactly $n - 1$.

Modular Addition I/O Degree = 2

Quadratic. More importantly: Quadratic I/O without extra variables

(the c_i can be all eliminated)

$$(*)\begin{cases} z_0 = x_0 + y_0 \\ z_1 = x_1 + y_1 + c_1 \\ z_2 = x_2 + y_2 + c_2 \\ \vdots \\ z_i = x_i + y_i + c_i \\ \vdots \\ z_{n-1} = x_{n-1} + y_{n-1} + c_{n-1}, \end{cases}$$

$$(*')\begin{cases} c_1 = x_0 y_0 \\ c_2 = x_1 y_1 + (x_1 + y_1) c_1 \\ \vdots \\ c_i = x_{i-1} y_{i-1} + (x_{i-1} + y_{i-1}) c_{i-1} \\ \vdots \\ c_{n-1} = x_{n-2} y_{n-2} + (x_{n-2} + y_{n-2}) c_{n-2} \end{cases}$$

MC (+ Mod 2^n) = n-1

Theorem 6.1.1. The Multiplicative Complexity (MC) of the addition modulo 2^n is exactly $n-1$.

Proof:

we have:

$xy + (x + y)c = (x + c)(y + c) - c^2$

1x each

$$x_0 y_0$$

$$x_1 y_1 + (x_1 + y_1) c_1$$

$$x_{i-1} y_{i-1} + (x_{i-1} + y_{i-1}) c_{i-1}$$

$$= x_{n-2} y_{n-2} + (x_{n-2} + y_{n-2}) c_{n-2}$$

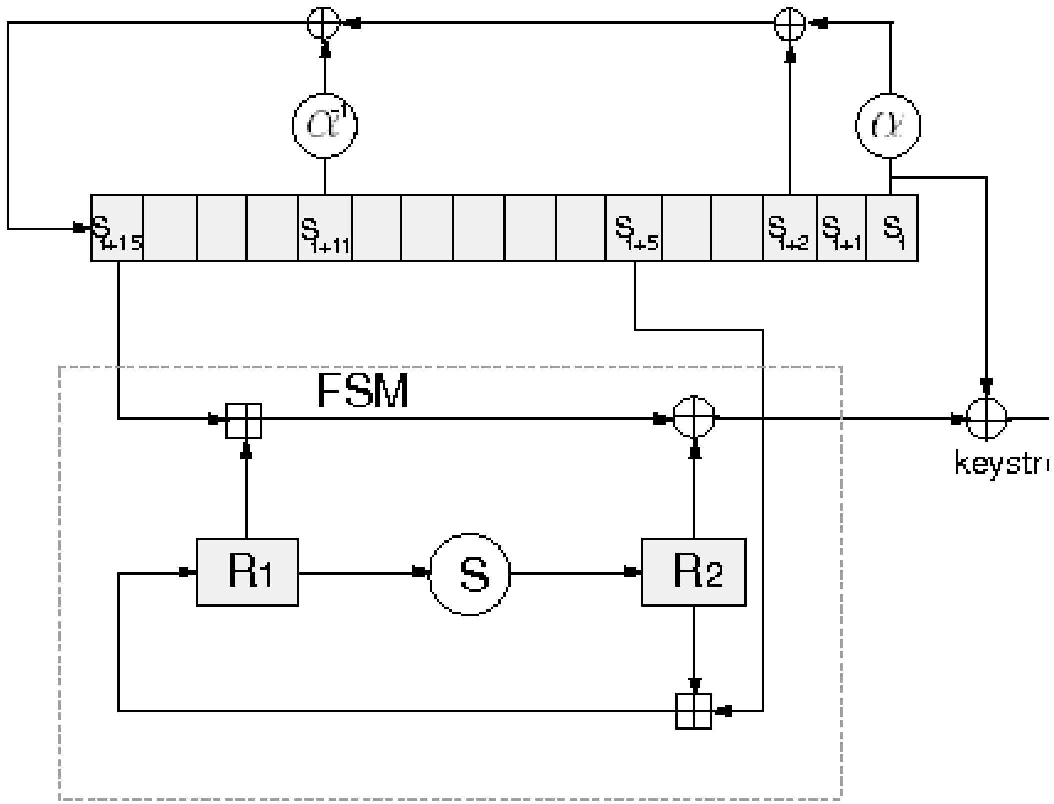
4.7. High-Level Attacks on Snow 2.0.

[Courtois-Debraize ICICS 2008]

Snow 2.0. [Courtois-Debraize ICICS 2008]

We analyse the keystream generator only, as a cipher with 576 key bits.

Any attack faster than 2^{576} is interesting…



Conditional algebraic attacks:

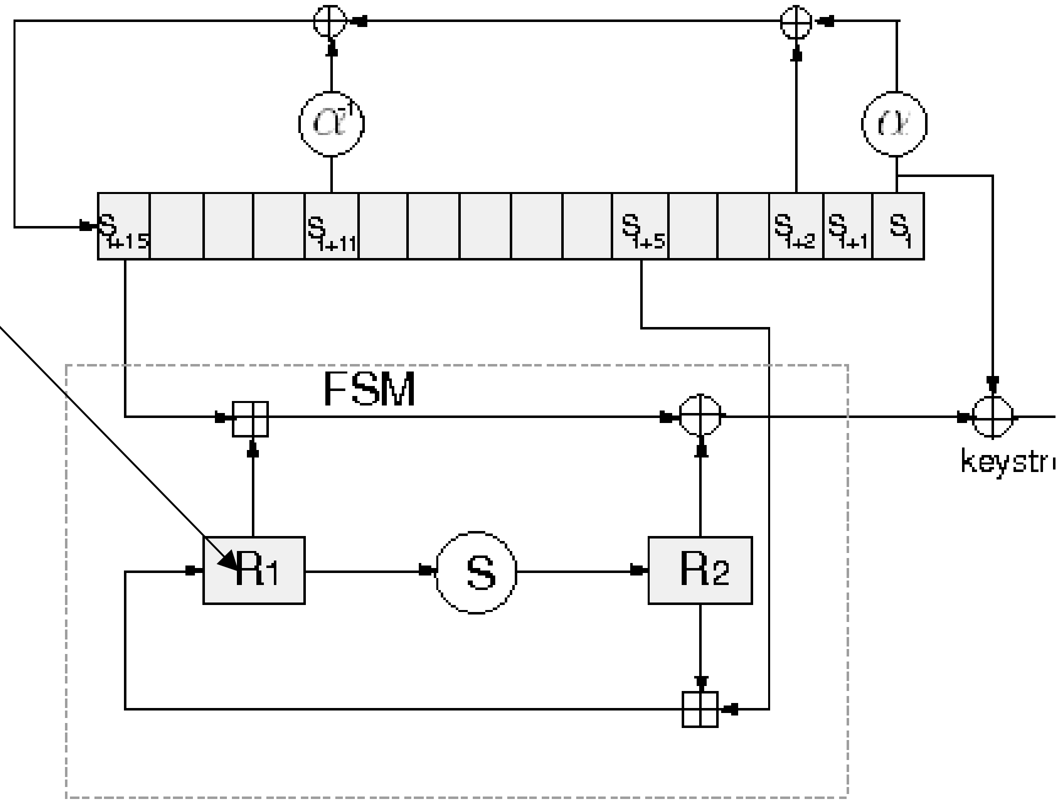
Amplification:

- given n linear assumptions,
  get C*n consequences.
  - Find attacks that maximize C!
  - A precise measure of “structural” algebraic vulnerability.
- 2x for + mod 2^n.
- 4x for Snow 2.0. Keystream generator.
  – Non-trivial result and method…

Amplification=4 or How to Linearize Snow?

Fix to 0.

For 9 consecutive steps.



Linearizes both +!

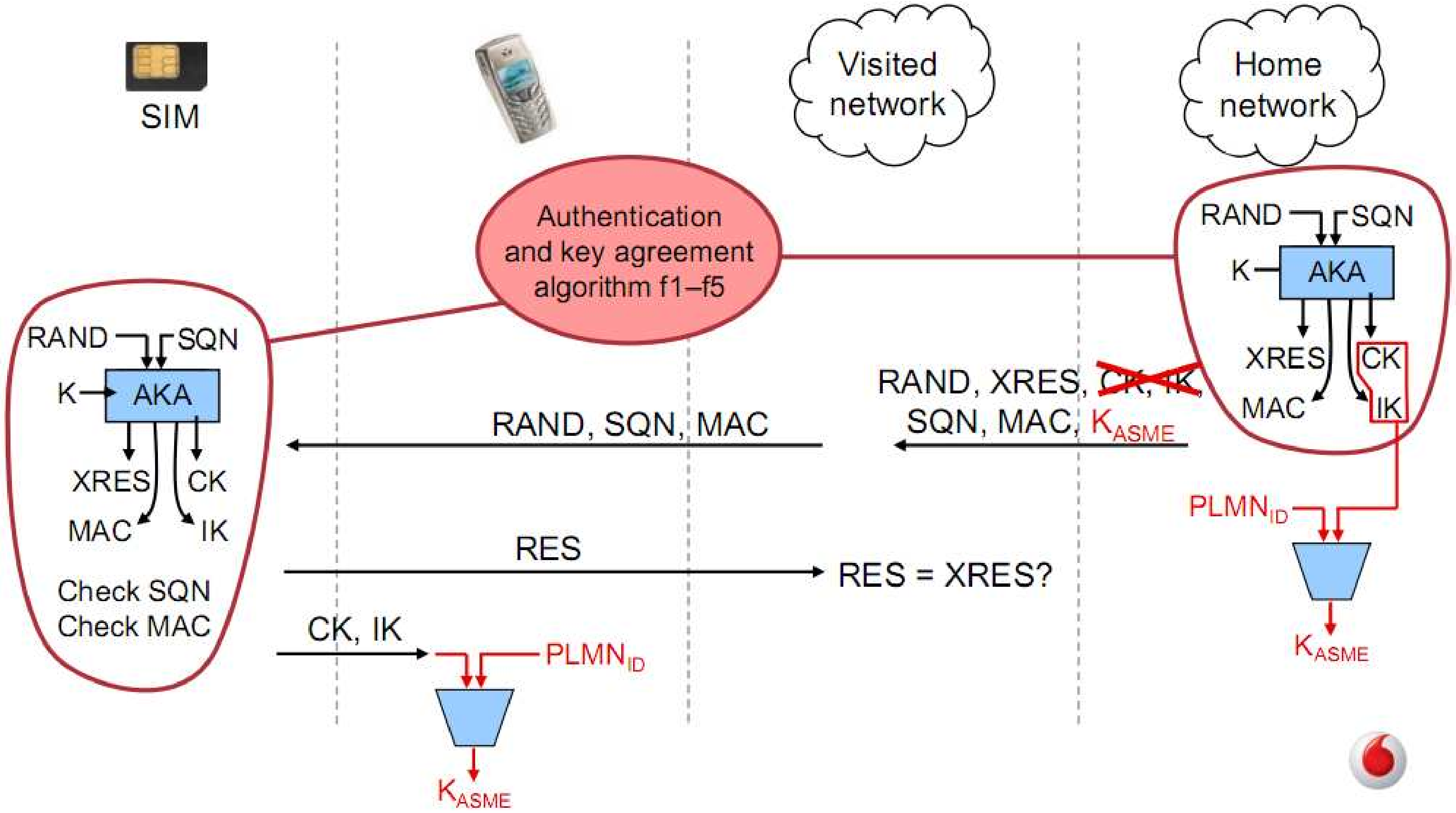
And the S-box layer

n -> 4n equations.

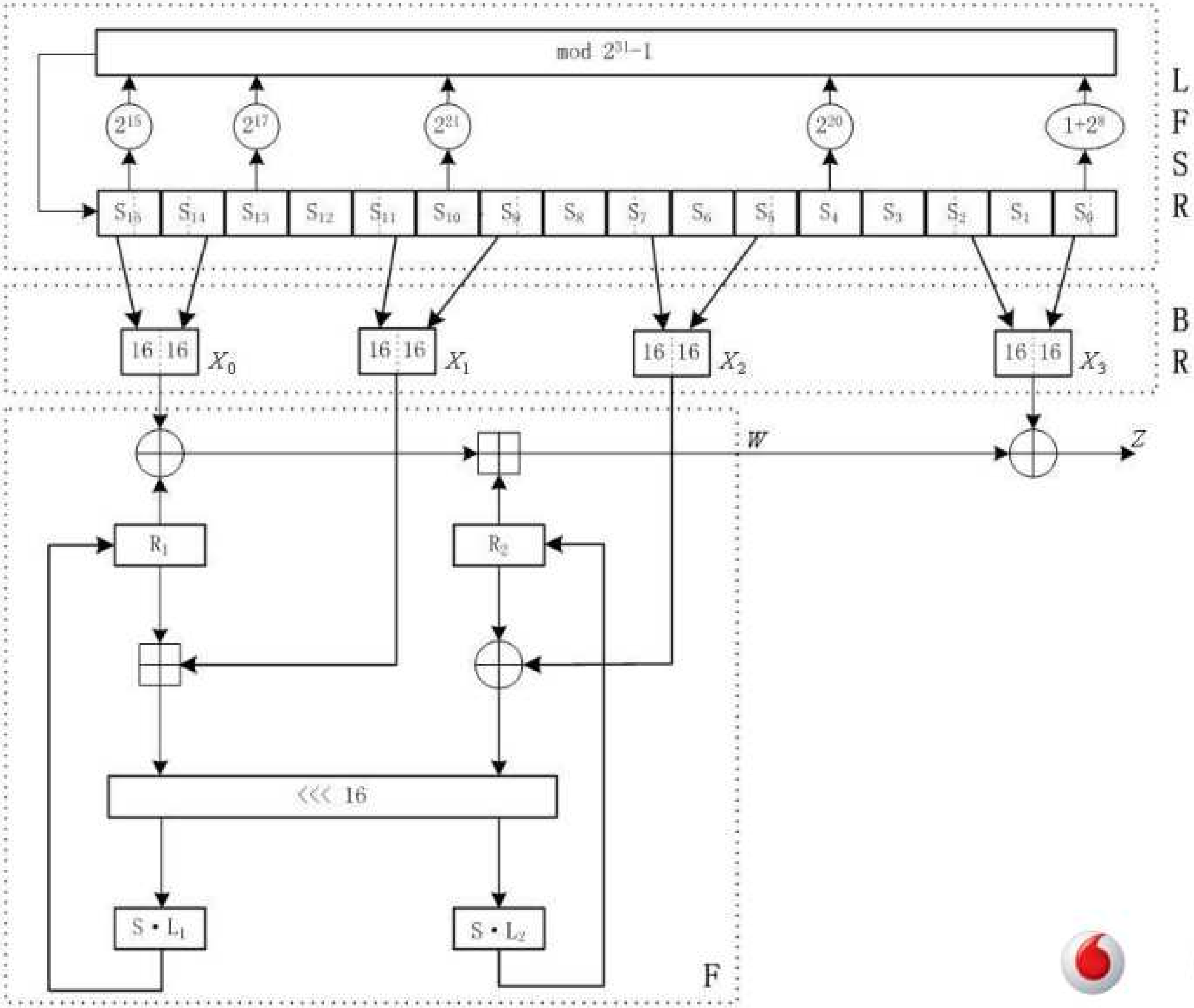
Seems optimal.

4.8. Variants of Snow 2.0. Sosemanuk, ZUC, etc.

**4G Telephony / LTE: Chinese Variant of Snow



**ZUC Cipher in 4G



$$\pi \approx {}^{355}/_{113}$$

Zu Chongzhi
[429-500]
祖冲之

5. GOST Cipher

GOST 28148-89

- The Official Encryption Standard of Russian Federation.
- Developed in the 1970s, or the 1980s,
  - First "Top Secret" algorithm.
  - Downgraded to "Secret" in 1990.
- Declassified in 1994.

Why Declassified

- 1994:
  - Shortly after the dissolution of the USSR, in a very troubled period where locations of nuclear weapons were sold for 5 $, it was indeed declassified and released to the public.
  - By mistake???
  - No country ever declassified their national algorithm.
    - In the UK no journalist would ever write anything about UK or NATO cryptography, due to so called DA-Rules
      - (BTW. Russia, China, Japan is not in NATO)
      - Secret algorithms, never made public, not even 50 years later…

Applications of GOST

- Much cheaper to implement than DES, AES and any other known cipher… (details later).

- Widely implemented and used:
  - Crypto ++,
  - Open SSL,
  - RSA Labs, Etc.
  - Central Bank of Russia,
  - other very large Russian banks..

GOST vs. DES

We hear that: “GOST 28147 “was a Soviet alternative to the United States standard algorithm, DES”

- ???? this is just wrong:
- very long key, 256 bits, military-grade
  - in theory secure for 200 years…
  - not a commercial algorithm for short-term security such as DES…

Can GOST be Used to Encrypt Secret documents?

United States DES
can be used ONLY for unclassified documents.

In contrast,

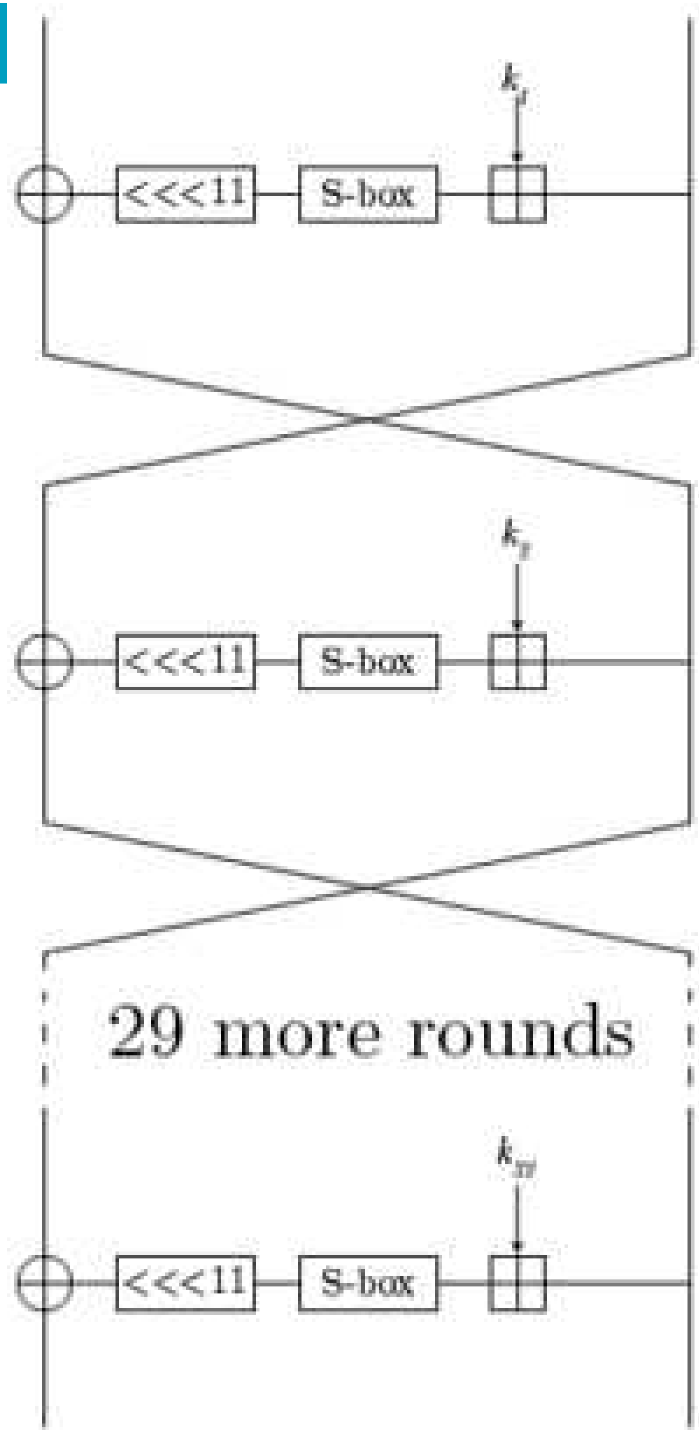
from the English preface to a translation of the Russian standard, by Aleksandr Malchik and Whitfield Diffie, Link:

193.166.3.2/pub/crypt/cryptography/papers/gost/russian-des-preface.ps.gz

GOST "does not place any limitations on the secrecy level of the protected information".

GOST

- Key = 2^{256} initial settings.
- S-boxes = 2^{512} possibilities.
  - But if bijective 2^{354} possibilities.
- Total 2^{610} (or 2^{768}).
  - Compare to 2^{151} possibilities with FIALKA.



GOST Boxes

- 8 secret S-boxes. (354 bits of info)
  - Central Bank of Russia uses these: →
- Secret S-boxes
  are the equivalent
  of secret rotors in FIALKA

#	S-Box
1	4 10 9 2 13 8 0 14 6 11 1 12 7 15 5 3
2	14 11 4 12 6 13 15 10 2 3 8 1 0 7 5 9
3	5 8 1 13 10 3 4 2 14 15 12 7 6 0 9 11
4	7 13 10 1 0 8 9 15 14 4 6 12 11 2 5 3
5	6 12 7 1 5 15 13 8 4 10 9 14 0 3 11 2
6	4 11 10 0 7 2 1 13 3 6 8 5 9 12 15 14
7	13 11 4 1 3 15 5 9 0 10 14 7 6 8 2 12
8	1 15 13 0 5 7 10 4 9 2 3 14 6 11 8 12

- Our attacks work
  for any S-boxes
  but they must be known.
  - there are methods about how to recover the secret S-boxes…

Analysis of GOST

- It was analysed by Schneier, Biham, Biryukov, Dunkelman, Wagner, Pieprzyk, Gabidulin,…
- Nobody found an attack…

Research on GOST

Before 2010 there were many papers on

- weak keys in GOST,
- attacks for some well-chosen number of rounds [Kara,some sliding attacks],
- attacks with modular additions removed [Biryukov-Wagner]
- related-key attacks [Kelsey,LucksFleischmann,Russian rebuttal]
- reverse engineering attacks on S-boxes [Saarinen,Furya]
- and collision and pre-image attacks on the hash function based on this cipher [Mendel,Szmidt et al.].

In all these attacks the attacker had much more freedom than we allow ourselves.

*Claims on GOST

Wikipedia April 2011:

Cryptanalysis of GOST

Compared to DES, GOST has a very simple round function. However, the designers of GOST attempted to offset the simplicity of the round function by specifying the algorithm with 32 rounds and secret S-boxes.

Another concern is that the avalanche effect is slower to occur in GOST than in DES. This is because of GOST's lack of an expansion permutation in the round function, as well as its use of a rotation instead of a permutation. Again, this is offset by GOST's increased number of rounds.

There is not much published cryptanalysis of GOST, but a cursory glance says that it seems secure (Schneier, 1996).

The large number of rounds and secret S-boxes makes both linear and differential cryptanalysis difficult. Its avalanche effect may be slower to occur, but it can propagate over 32 rounds very effectively.

[Biryukov, Wagner, Eurocrypt 2000]

“Even after considerable amount of time and effort, no progress in cryptanalysis of the standard was made in the open literature”

More [Biryukov, Wagner, Eurocrypt 2000]

"GOST looks like a cipher that can be made both arbitrarily strong or arbitrarily weak depending on the designer's intent since some crucial parts of the algorithm are left unspecified."

-----disagree, it seems that bijective S-boxes are always quite secure, even identity functions!

"A huge number of rounds (32) and a well studied Feistel construction combined with Shannon's substitution-permutation sequence provide a solid basis for GOST's security."

"However, as in DES everything depends on the exact choice of the S-boxes and the key-schedule."

NO YES!

5.2. GOST on the International Stage

Consensus on GOST Security [2010]

Axel Poschmann, San Ling, and Huaxiong Wang:
256 Bit Standardized Crypto for 650 GE – GOST Revisited,
In CHES 2010

"Despite considerable
cryptanalytic efforts
spent in the past 20 years,
GOST is still not broken."

Security + Implementation Or Why GOST is Very Competitive

Same paper: Axel Poschmann, San Ling, and Huaxiong Wang: 256 Bit Standardized Crypto for 650 GE – GOST Revisited, In CHES 2010

- GOST-PS, fully Russian standard compliant variant using the S-boxes taken from PRESENT cipher:
  - only 651 GE
- The Russian Central Bank version is called GOST-FB,
  - it requires 800 GE
- AES-128
  - requires 3400 GE for a much lower security level!
- DES
  - requires also about 4000 GE…
- PRESENT: 1900 GE for 128-bit version.

in terms of cost/security level claimed GOST is probably strictly the best symmetric cipher known…

GOST and International Standards Organization [ISO]

ISO

- Less than 10 crypto algorithms were ever standardized by ISO. E.g. AES.
- All in ISO 18033.
  - Four 64-bit block ciphers:
    - TDES, MISTY1, CAST-128, HIGHT
  - Only three 128-bit block ciphers:
    - AES, Camellia, SEED

GOST in ISO

- In 2010 GOST was also submitted to ISO 18033 to become an international standard.
- In the mean time GOST was broken.
- Two attacks were published in early 2011:
  - One by Takanori Isobe [FSE 2011].
  - One by Nicolas Courtois [eprint/2011/211].

Finally..

GOST was rejected at ISO

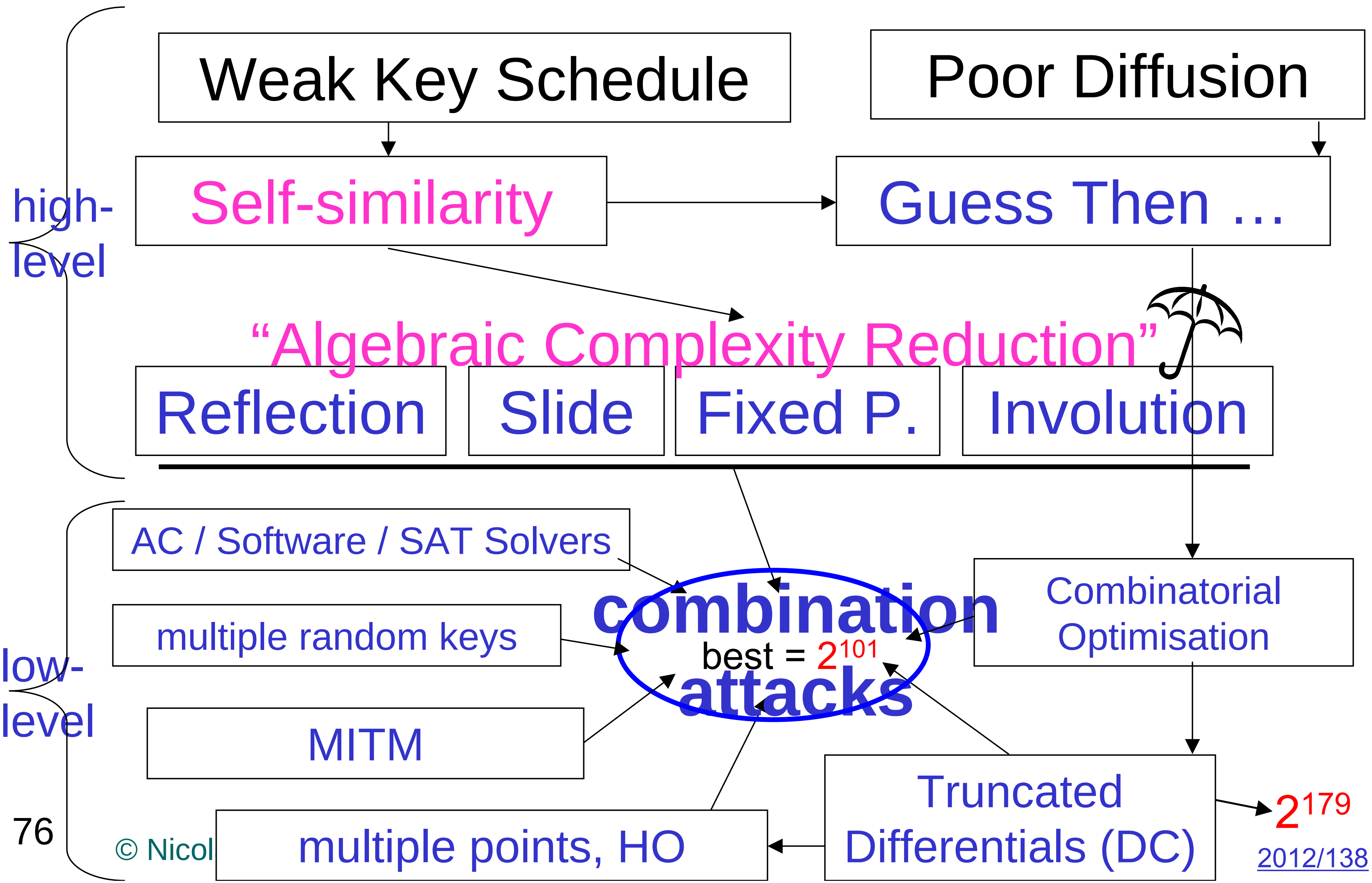
- by a majority vote

Future of GOST in ISO

- Our report [eprint/2011/211] was officially submitted to ISO.
- It says: […] to standardize GOST now would be really dangerous and irresponsible […]
- Why?
  – Half-broken in very serious sense
  – Really broken in academic sense

What's Wrong? >50 distinct attacks… Best = 2^{101}

cf. 2011/626



6. Algebraic Complexity Reduction

Conditional AC

<u>Definition</u> [informal on purpose] Methods to substantially reduce the size of and the complexity of equations that appear throughout the computations…

$\Rightarrow$ Very rich galaxy of attacks to be studied in the next 20 years…

How to lower the degree ?

- By adding new equations
- Which split the system into pieces and decrease the number of rounds

} conditional AC…

[Black Box] Reduction Paradigm

Black-box
- high-level
- guess and determine methods
- which transform
- an attack … into another…

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.

Some 40 distinct reductions of this type with a large variety of X,Y, Z, T can be found in

eprint/2011/626

Example

- Given 2^{32} KP for the full 32-round GOST.
- Obtain 4 KP for 8 rounds of GOST.
- This valid with probability 2^{-128}.

Is Algebraic Complexity Reduction Already Known?

There exists many known attacks which enter the framework of Algebraic Complexity Reduction:

- Slide attacks
- Fixed Point Attacks
- Cycling Attacks
- Involution Attacks
- Guessing [Conditional Algebraic Attacks]
- Etc..

What's New?

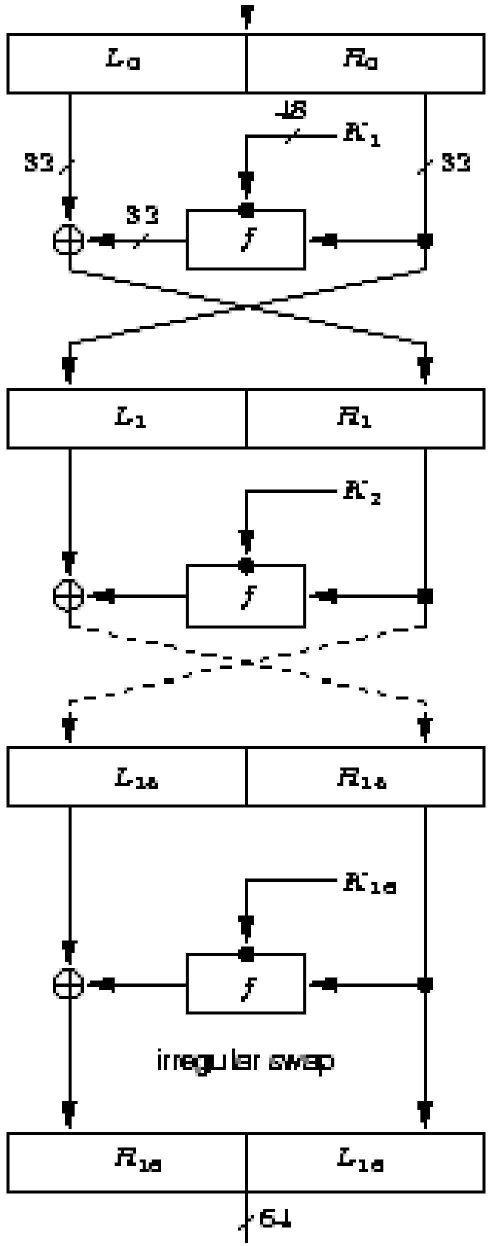
Slide / Fixed Point / Cycling / Guessing / Etc..

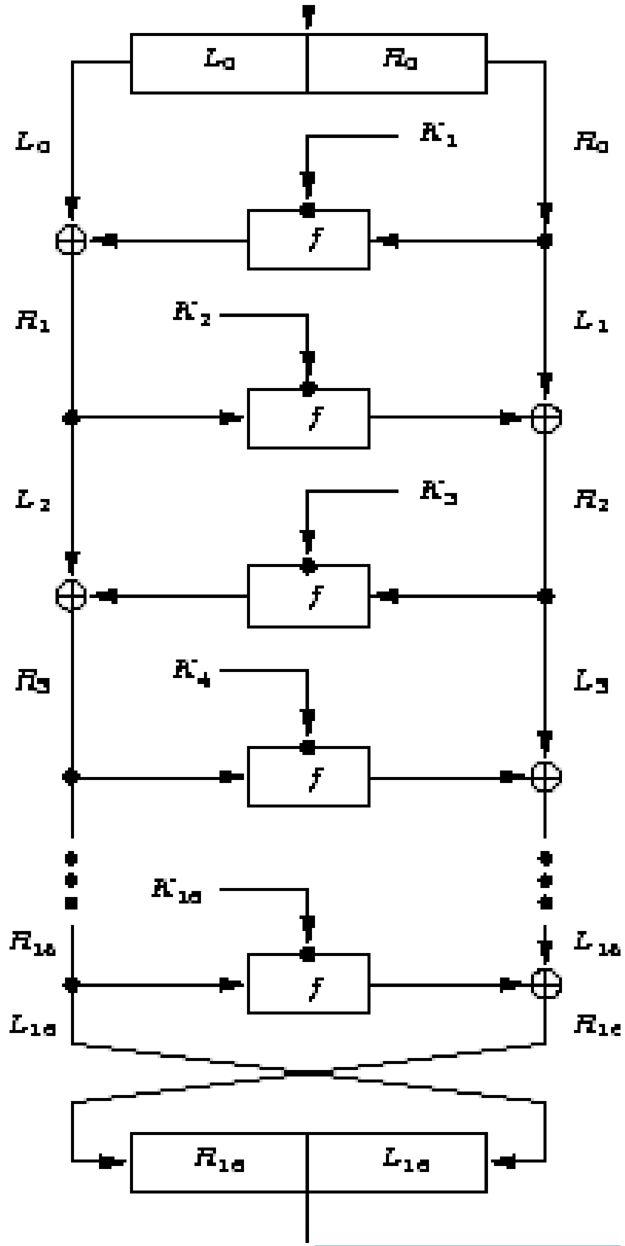
WHAT'S NEW?

- There are now many completely new attacks which are exactly none of the above [though similar or related].
- Many new attacks are possible and many of these attacks were never studied 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 attack [e.g. algebraic, MITM].

Revision:
Feistel Schemes

2x Same


L_0
R_0
48
K_1
33
33
33
f
L_1
R_1
K_2
L_{16}
R_{16}
K_{16}
irregular swap
R_{16}
L_{16}
64


L_0
R_0
K_1
R_1
L_1
K_2
L_2
R_2
K_3
R_3
L_3
K_4
K_{16}
R_{16}
L_{16}
f
R_{16}
L_{16}

6.2. Structure of GOST

$$Enc_k = \mathcal{D} \circ \mathcal{S} \circ \mathcal{E} \circ \mathcal{E} \circ \mathcal{E}$$

Self-Similar Key Schedule
Periodic Repetition + Inversed Order

rounds	1 … 8	9 … 16	17 … 24	25 … 32
keys	$\mathbf{k}_0 k_1 k_2 k_3 k_4 k_5 k_6 k_7$	$\mathbf{k}_0 k_1 k_2 k_3 k_4 k_5 k_6 k_7$	$\mathbf{k}_0 k_1 k_2 k_3 k_4 k_5 k_6 k_7$	$k_7 k_6 k_5 k_4 k_3 k_2 k_1 \mathbf{k}_0$

Table 1. Key schedule in GOST

We write GOST as the following functional decomposition (to be read from right to left) which is the same as used at Indocrypt 2008 [29]:

$$Enc_k = \mathcal{D} \circ \mathcal{S} \circ \mathcal{E} \circ \mathcal{E} \circ \mathcal{E} \quad (1)$$

Where $\mathcal{E}$ is exactly the first 8 rounds which exploits the whole 256-bit key, $\mathcal{S}$ is a swap function which exchanges the left and right hand sides and does not depend on the key, and $\mathcal{D}$ is the corresponding decryption function with $\mathcal{E} \circ \mathcal{D} = \mathcal{D} \circ \mathcal{E} = Id$.

*Compare: DES

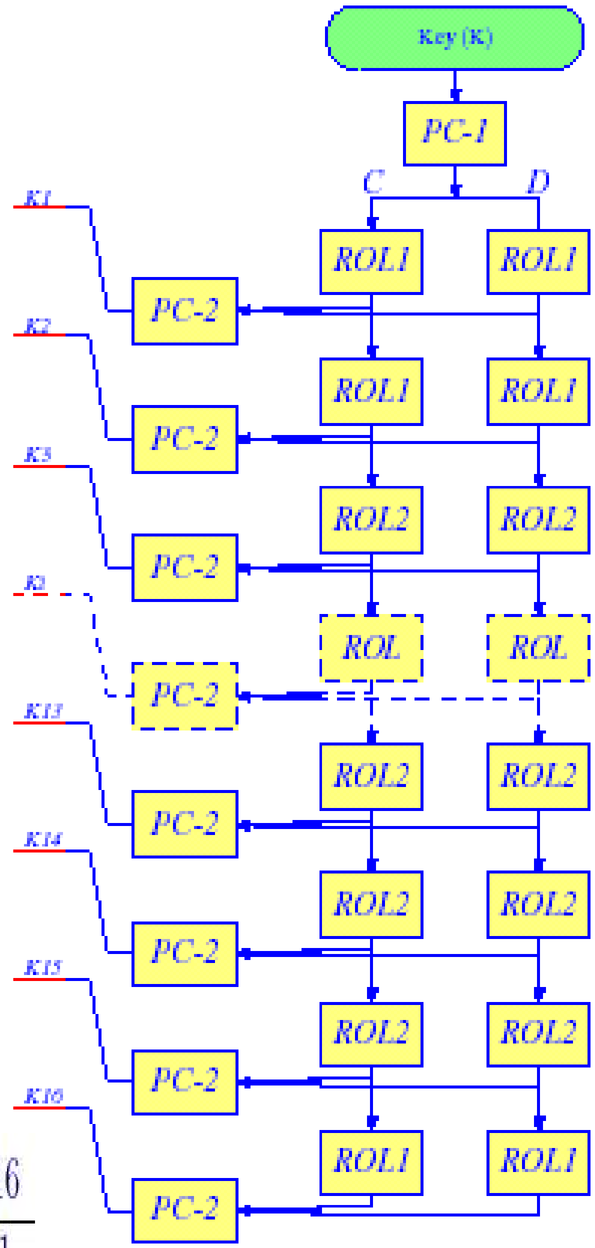
PC1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
above for C_i; below for D_i						
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

16*48 subsets of 56 bits.

1: $K \xrightarrow{\text{PC1}} (C, D)$
2: **for** $i = 1$ to 16 **do**
3: $\quad C \leftarrow \text{ROL}_{r_i}(C)$
4: $\quad D \leftarrow \text{ROL}_{r_i}(D)$
5: $\quad K_i \leftarrow \text{PC2}(C, D)$
6: **end for**

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
r_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1



Fixed Points: DES Key Schedule

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
r_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

R1 R8 R15

- Can DES key be periodic?
- After step 1= key for R1
- After step 8=key for R8
- After step 15=key for R15
- We have a pattern G of length 7 which repeats twice.
- Unhappily G = + 13 mod 28 (and not 14)
- Does NOT have many fixed points.

Last 16 Rounds of GOST

$$Enc_k = \boxed{\mathcal{D} \circ \mathcal{S} \circ \mathcal{E}} \circ \mathcal{E} \circ \mathcal{E}$$

"Theorem Which Won World War 2",

[I. J. Good and Cipher A. Deavours, afterword to: Marian Rejewski, "How Polish Mathematicians Deciphered the Enigma", Annals of the History of Computing, 3 (3), July 1981, 229-232]

P and

Q^{-1} o P o Q

have the same cycle structure

Last 16 Rounds of GOST

$$Enc_k = \boxed{\mathcal{D} \circ \mathcal{S} \circ \mathcal{E}} \circ \mathcal{E} \circ \mathcal{E}$$

$\longleftarrow$

"Theorem Which Won World War 2",

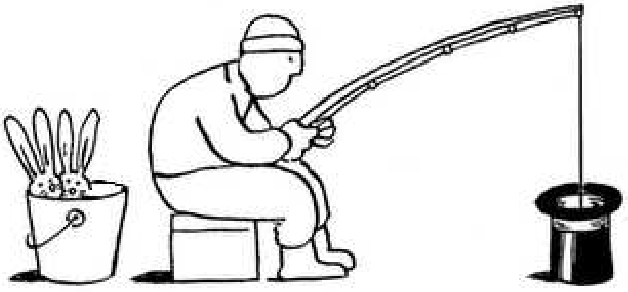
$\Rightarrow$ Has exactly 2^{32} fixed points (order 1) and 2^{64}-2^{32} points of order 2.

$\Rightarrow$ A lot of fixed points (very few for DES).

6.3. Complexity Reduction in Guess-Then-Determine attacks

Reason: Self-Similarity

6.3.1. Guess-Then-Determine: Amplification



Amplification

Definition 3.2.1 (Amplification, Informal). The goal of the attacker is to find a reduction where he makes some assumption at a certain initial cost, for example they are true with probability 2^{-X} or work for certain proportion 2^{-Z} of keys. Then the attacker can in constant time determine many other internal bits inside the cipher to the total of Y bits.
We call amplification the ratio $A = Y/X$.

We are only interested in cases in which the values X and Z are judged realistic for a given attack, for example $Z < 32$ and $X < 128$.

Killer examples:

- Slide attacks – unlimited.
- Weak Key Family 3 in GOST – VERY large amplification => attack on GOST with 2^{159} per key

6.4. Complexity Reduction: First Example:

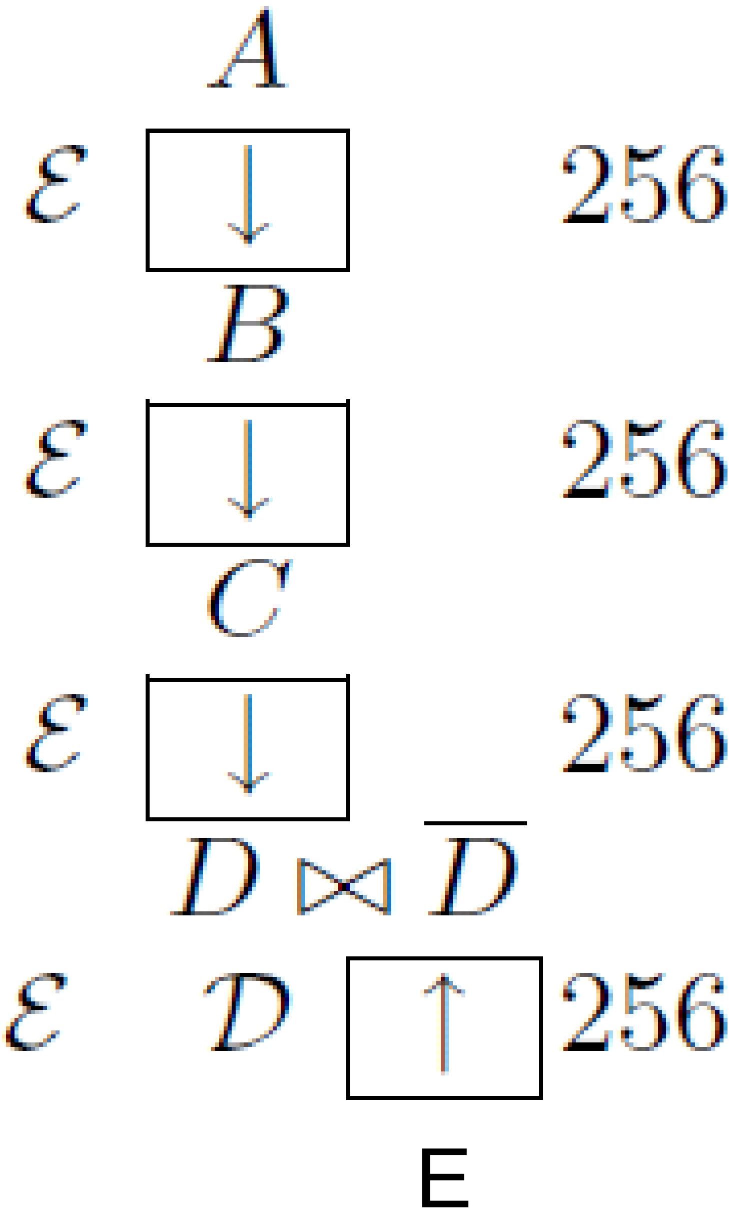
Relaxing the Requirements of A Sliding Attack

Black Box Reduction: Pseudo-Sliding Attack

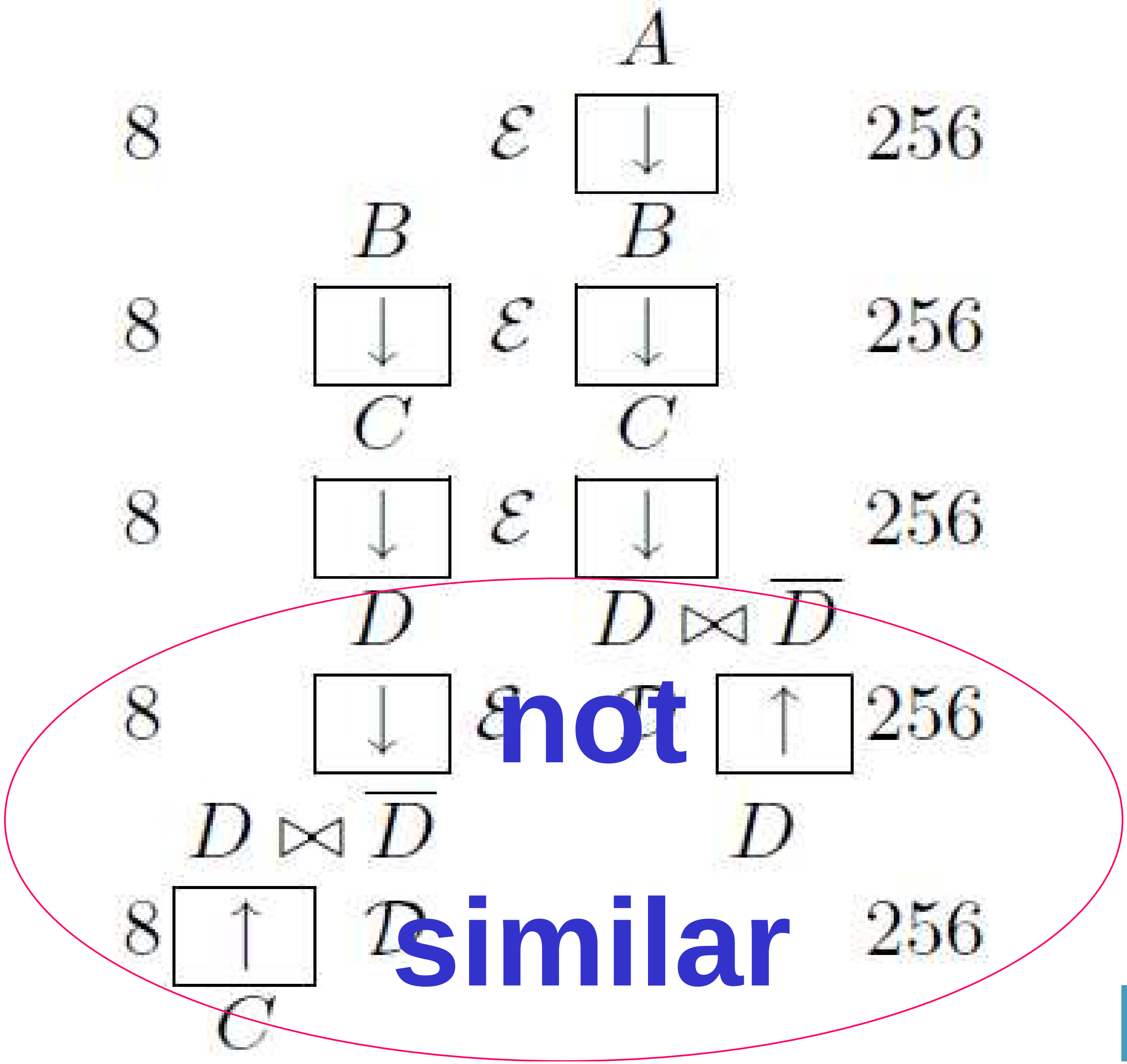
[Cryptologia Jan 2012]

One Encryption

$$Enc_k = \mathcal{D} \circ \mathcal{S} \circ \mathcal{E} \circ \mathcal{E} \circ \mathcal{E}$$



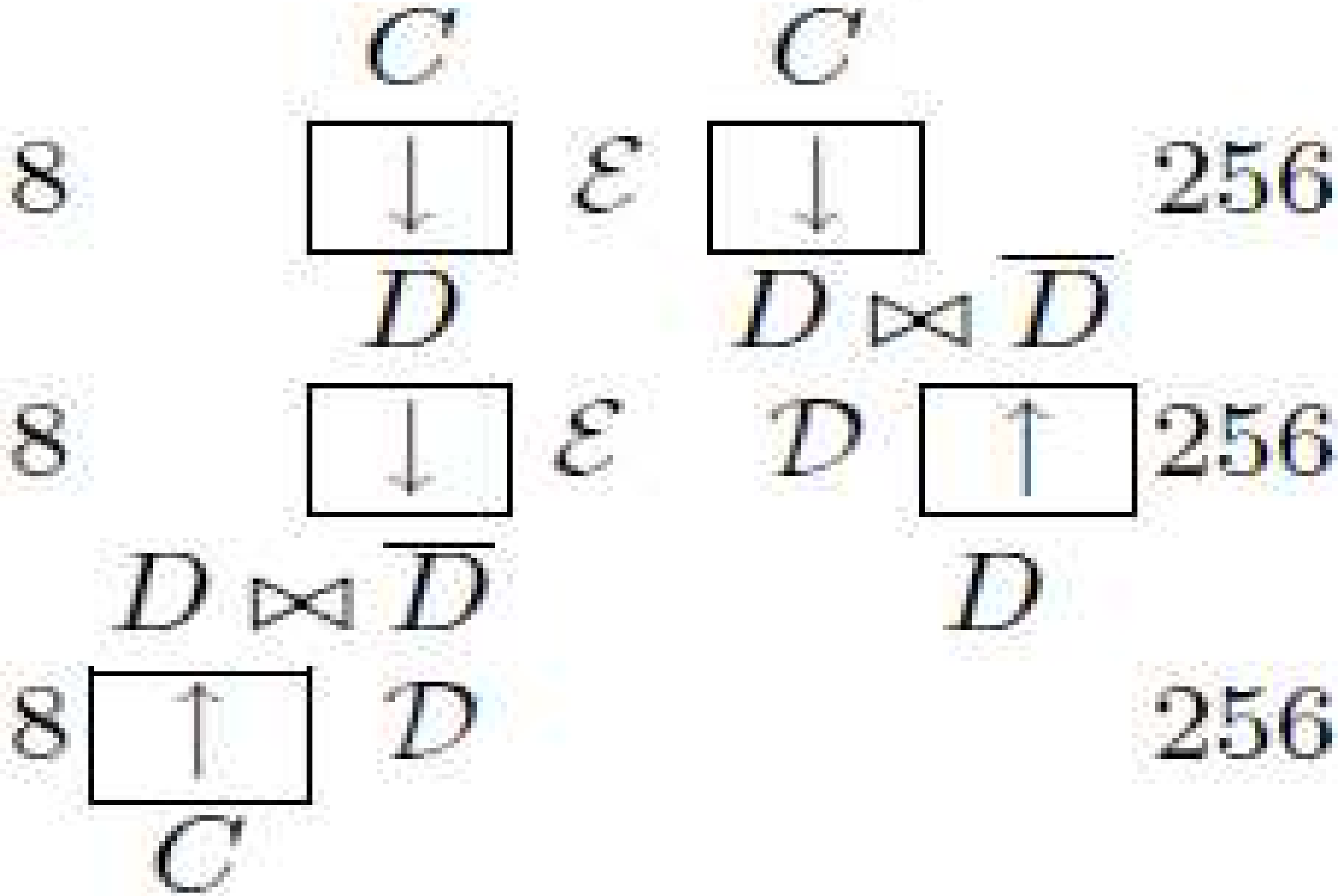
Two Encryptions with A Slide

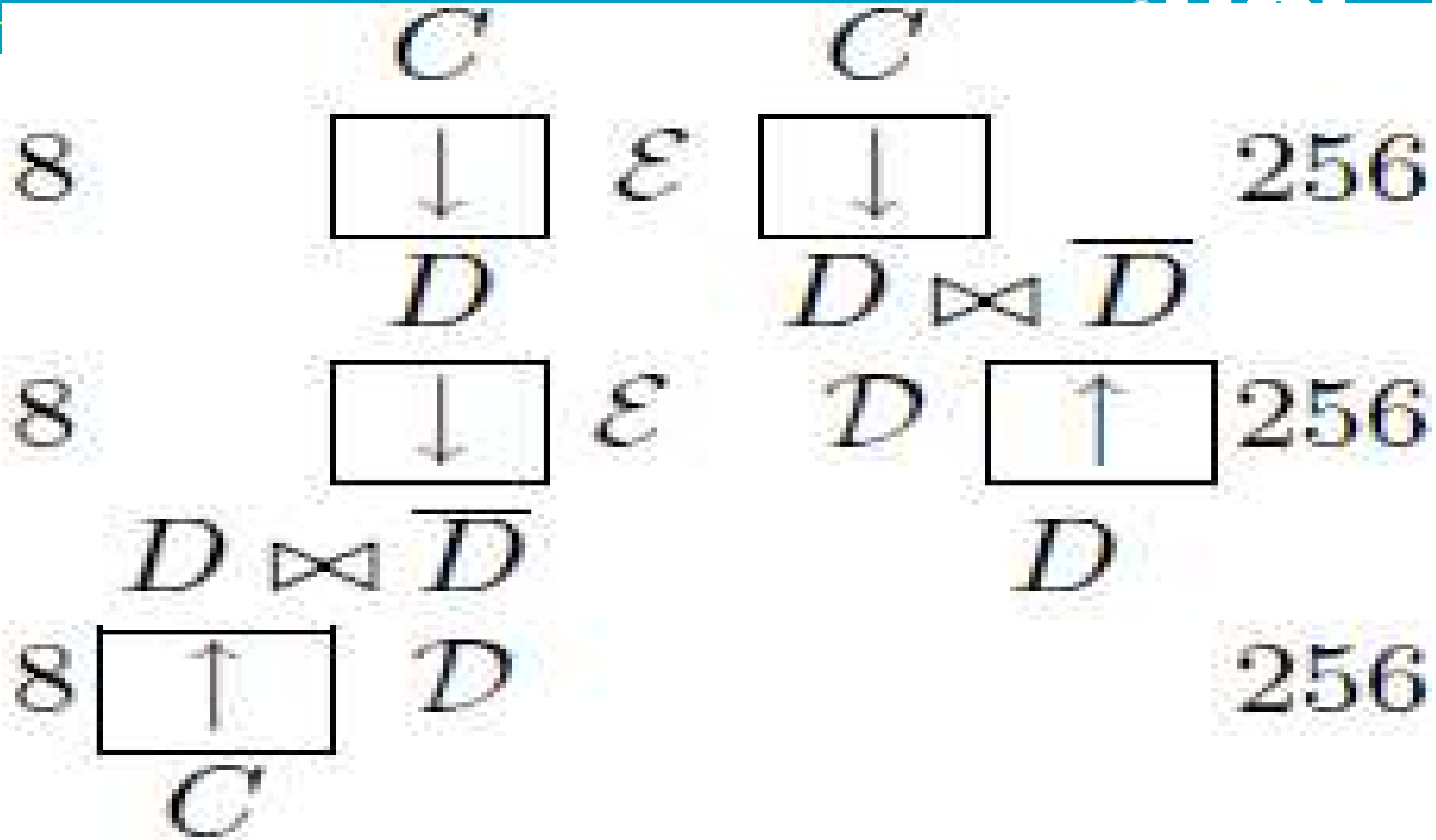


Assumptions

We proceed as follows. We consider plaintexts with a very peculiar property:

Assumption 1 (Assumption W). Let A be such that $\mathcal{E}(D) = \overline{D}$ where D is defined as $D = \mathcal{E}^3(A)$.





Fact 2 (Property W). Given 2^{64} KP there is on average one value A which satisfies the Assumption. For 63% of all GOST keys at least one such A exists.

Remark: For the remaining 37 % of keys this attack fails. However many other attacks still work, see [12].

Reduction

New Attack on GOST

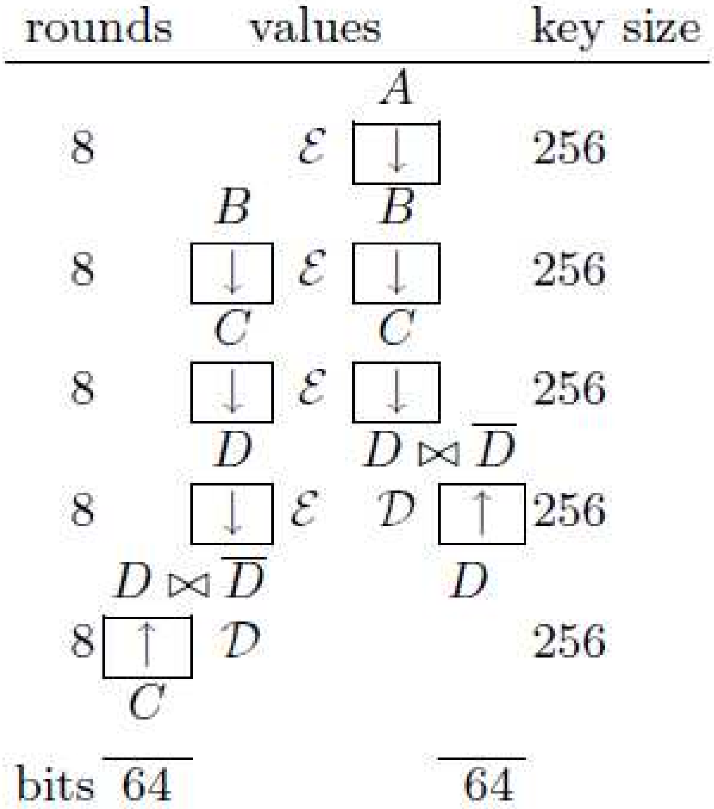
Fact 3 (Consequences of Property W). If A satisfies the Assumption W above and defining $B = \mathcal{E}(A)$ and $C = \mathcal{E}(B)$ we have:

1. $Enc_k(A) = D$. This is illustrated on the right hand side of Fig. 1.
2. $Enc_k(B) = C$ This can be seen on the left hand side of Fig. 1.

2^{64} KP

guess A,B

correct $P=2^{-128}$



$P=2^{-128}$

=>

4 pairs

for 8 rounds

Fig. 1. A black-box "Algebraic Complexity Reduction" from 32 to 8 rounds of GOST

Final Key Recovery 8R

4 Pairs, 8 rounds.

The key is found within

2^{94} GOST computations.

Overall Attack

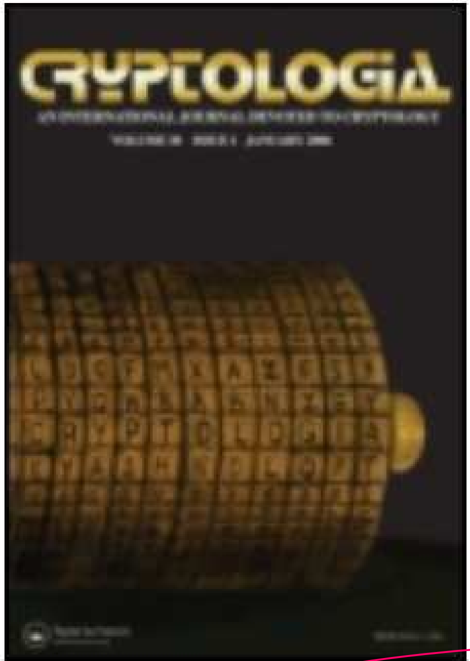
2^{128+94} GOST computations.

2^{33} times faster than brute force.

Not the best attack yet.

Cryptologia [Jan 2012]

Editorial:



Cryptologia

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

Space Crunchers and GOST Busters!

Craig Bauer

Available online: 12 Jan 2012

Finally, I welcome Nicolas T. Courtois to our pages. His paper attacking the GOST cipher is the first of several I hope to receive.

Best Wishes,
Craig Bauer
Editor-in-Chief

6.5. More Single Key Attacks…

Many more single-key attacks on full 32-round GOST…

cf. eprint.iacr.org/2011/626/

Reduction Summary					
Reduction cf.	Red. 1 §9.1	Red. 2 §10	Red. 3 §11	Red. 4 §11.1	Red 5 §12
Type	1x Internal Reflection		2x Reflection		Fixed Point
From (data 32 R)	2^{32} KP		2^{64} KP		
Obtained (for 8R)	**2** KP	**3** KP	**3** KP	**4** KP	**2** KP
Valid w. prob.	2^{-96}	2^{-128}	2^{-96}	2^{-128}	2^{-64}

Last step	MITM	Guess+ Det. Hybrid MITM-Software/Algebraic				
Cases ∈ Inside	2^{128}	2^{128}	2^{64}		2^{64}	2^{128}
Then Fact cf.	Fact 9	Fact 4	Fact 69		Fact 6	Fact 4
Time to break 8R	2^{128}	$2^{127}/2^{128}$	2^{110}		2^{94}	$2^{127}/2^{128}$
Storage bytes	2^{132}	$2^{39}/2^{46}$	-	2^{67}		$2^{39}/2^{46}$
♯ false positives	2^{224}		2^{192}	2^{128}		2^{192}
Attack time 32 R	2^{224}	$\mathbf{2^{223}}/2^{224}$	2^{228}	$\mathbf{2^{206}}$	2^{222}	$\mathbf{2^{191}}/2^{192}$

Science ≠ Politics

Main paper was submitted to Asiacrypt 2011.

One referee wrote: "I think that the audiences of Asiacrypt will not feel it is interesting."

=>however about half of papers accepted at this Asiacrypt are about things about which nobody ever heard, not even professional cryptologists (say JH42, Armadillo,theory, incremental research, things which would interest very few people)…, not to say it would interest anybody in the industry or government circles…

=>HOW many times it ever happened at Asiacrypt that a military-grade cipher, and an official government standard of a major country, used by large banks, implemented in SSL, was broken, while being in the process of being standardized by ISO to become a global industrial standard? Not many times.

⇒ impacting potentially all of: national critical infrastructures, key financial systems and even ordinary computer software

- ⇒ It could be worth tens of billions of dollars to fix problems due to GOST..
- ⇒ For now nothing bad happened, just some bad press.
  - ⇒ BUT: is GOST really broken?

Science ≠ Politics

But is GOST really so bad?

When it was submitted to ISO, and only then,
suddenly some cryptanalysts tried to break it… And succeeded.

And there is now more than 50 attacks… Academic attacks.

We do in “the West” ☺ put VERY HIGH super-paranoid requirements on security of ciphers…

- ⇒ It is debatable whether the Russian designers of GOST ever thought that it should not have attacks faster than 2^{256}…
- ⇒ Remember that GOST can have a secondary key: secret S-boxes.

Even today, in spite of all our 20+ attacks, GOST is better than any comparable cipher:

Look at the (best attack) / (implementation cost) ratio ← cf. Poschmann et al CHES 2010

- – Key schedule could be easily fixed to avoid academic shortcut attacks…
- – GOST-P is even better (better S-box <= PRESENT: new ISO standard).

6.6. Black Box Reduction: Reflection Attack

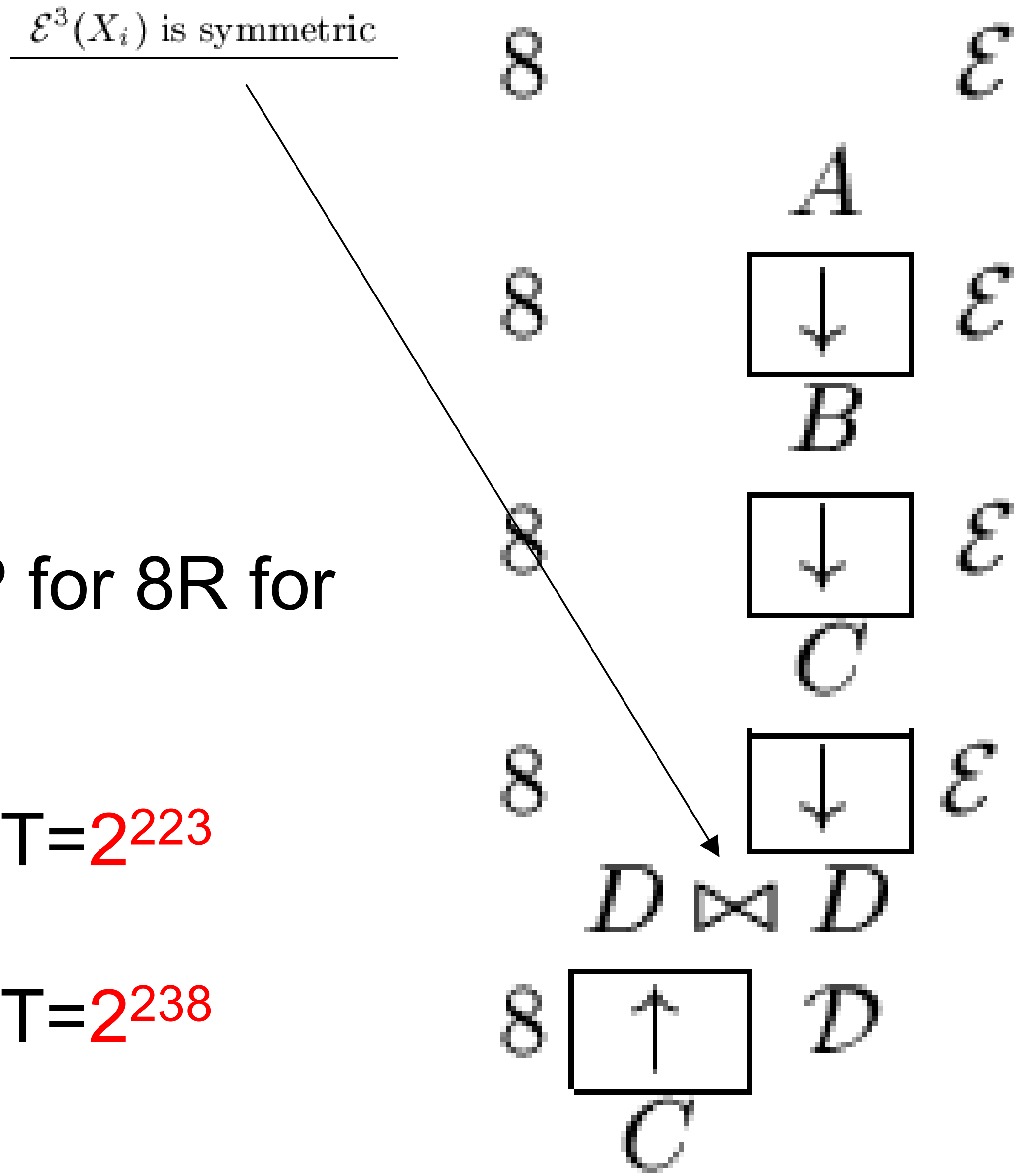
Reflection – Happens 2^{32} Times - KPA

- guess A det C
  info=64 cost=2^{-32}
- guess B
  info=64+64 cost=2^{-64}
- [guess D
  info=64 cost=2^{-32}]

Summary: we get 2/3 KP for 8R for the price of 2^{-96}/2^{-128}.

break 8R 2KP 2^{127}
=> break 32R D=2^{32} T=2^{223}

break 8R 3KP 2^{110}
=> break 32R D=2^{32} T=2^{238}



6.7. Double Reflection Attack

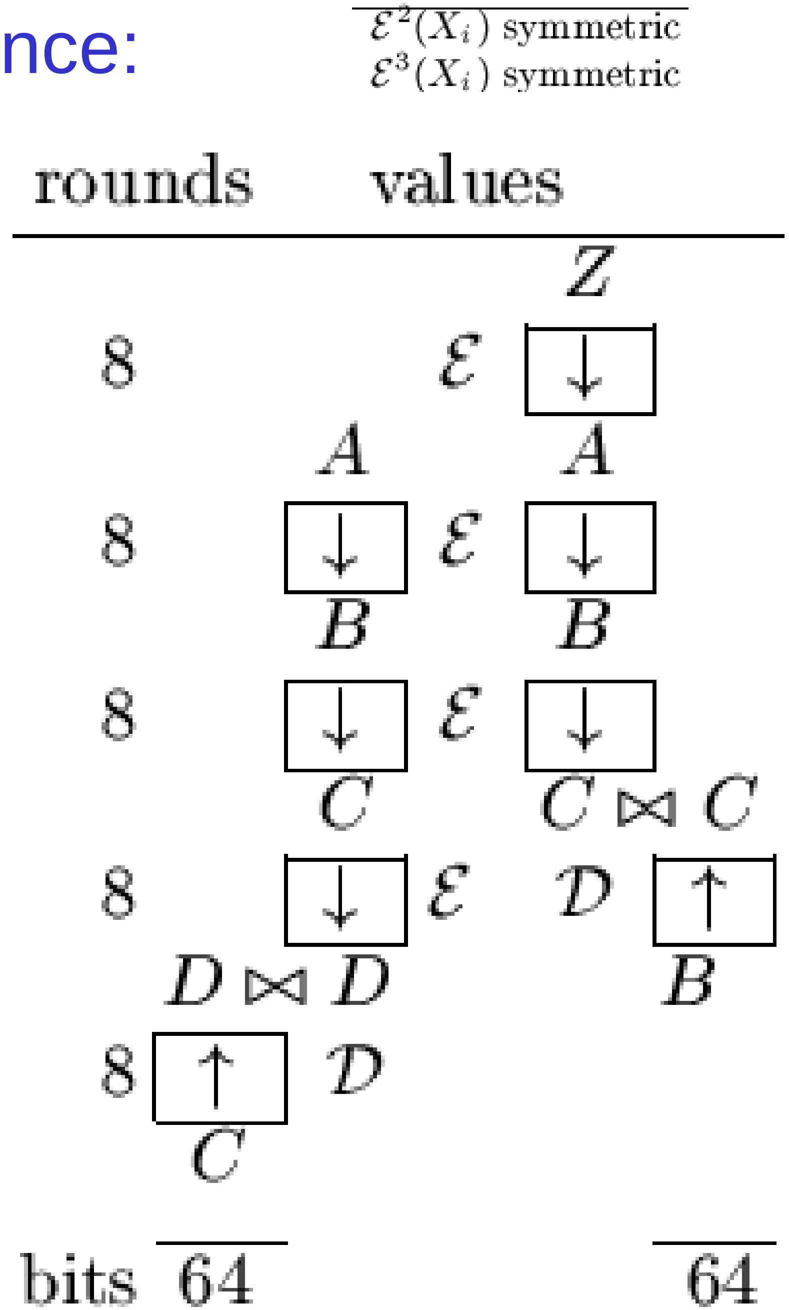
2x Reflection, Happens About Once:

- guess C det A
  info=64 cost=2^{-32}
- guess B det Z
  info=64+64+64 cost=2^{-64}
- [guess D
  info=64 cost=2^{-32}]

Summary: we get 3/4 KP for
8R for the price of $2^{-96}/2^{-128}$

break 8R 3KP 2^{110}
=> break 32R D=2^{64} T=2^{206}

break 8R 4KP 2^{94}
=> break 32R D=2^{64} T=2^{222}



Other Attacks?

Best single key attack:

D=2^{64} T=2^{179}

Nicolas Courtois: An Improved Differential Attack on Full GOST, March 2012, eprint.iacr.org/2012/138.

However ciphers are NEVER used with single keys in the real life… On the contrary.

7. Multiple Random Key Scenario

"stronger, more versatile
and MORE practical
than any known
single key attack"

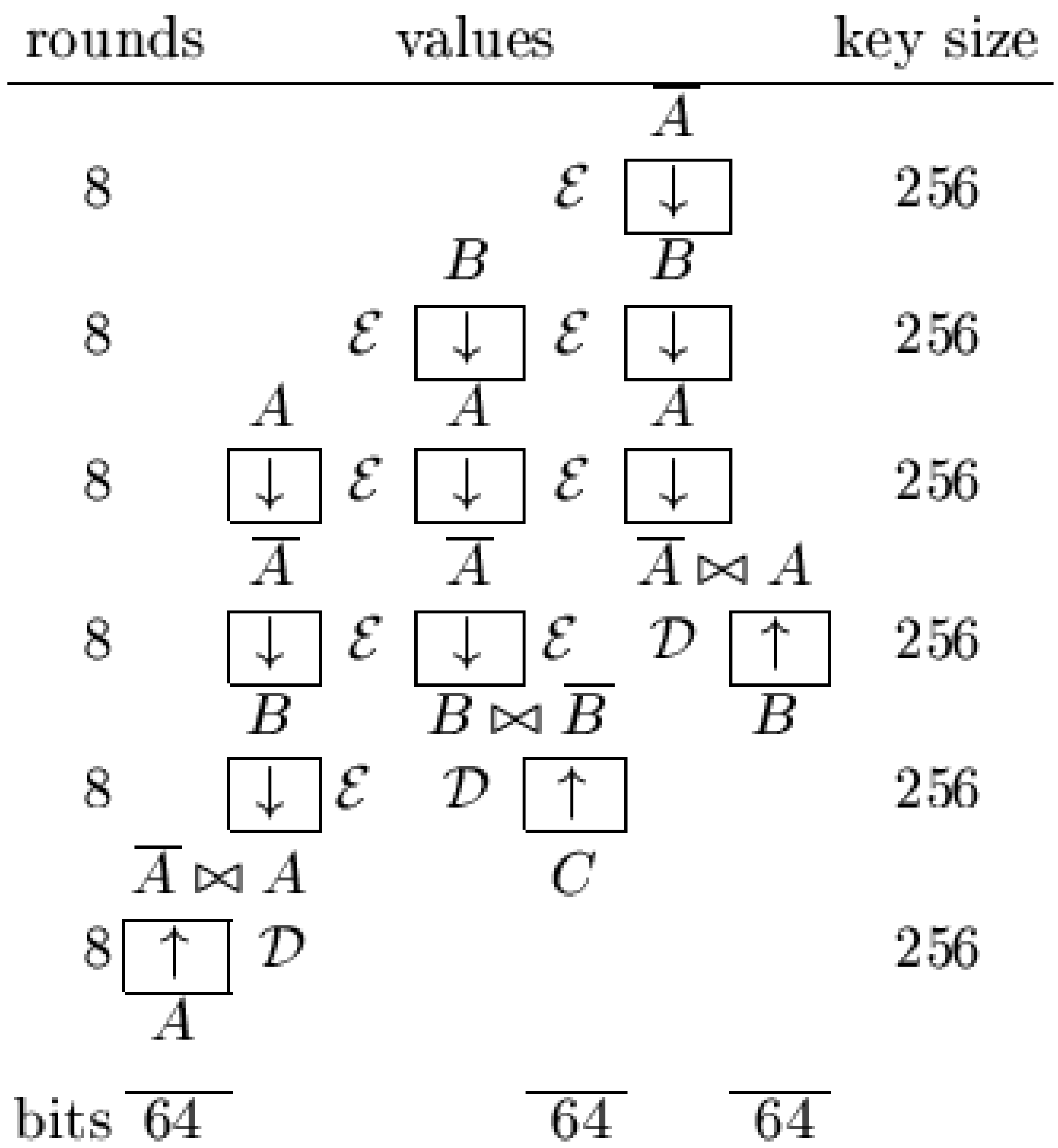
???

7.1. One Triple Reflection Attack

3x Reflection, Weak Keys 2^{-64}

$$\mathcal{E}^2(\overline{A}) = A$$

$$\mathcal{E}(A) = \overline{A}$$



No guessing =>

Very high amplification.

All data obtained nearly "for free".

8. Combined Attacks: DC + Algebraic Complexity Reduction

two totally unrelated families of attacks…
…until December 2012

New Combined Attacks

New attacks from November 2012 combine ALL of truncated differentials, fixed points, advanced MITM, software/SAT solvers and reflection in ONE single attack. Example:

Family 5.3. Fact 47 Section 19.5.

Given 2^{52} devices with random keys on 256 bits and 2^{32} ACP (Adaptively Chosen Plaintexts), we can recover one GOST key in time of 2^{139}.

Total data = 2^{84}. Mostly used to reject keys which do not satisfy our conditions.

8.1.
GOST and DC

…DC is yet another form of self-similarity (!)

GOST vs. LC and DC

Bruce Schneier, Applied Cryptography, 1996,
Section 14.1. page 334

"Against DC and LC,
GOST is probably stronger than DES"

Gabidulin 2000-2001:

7 rounds are sufficient
to protect GOST against DC.

8.1.2.
DC With Sets

Advances Differential Cryptanalysis of GOST

[Seki, Kaneko SAC 2000]:

Some 13 rounds out of 32 broken…

Sets of differentials = most general formulation

Incomplete/truncated Differentials = With free bits…

Sets Of Differentials [Seki-Kaneko,Courtois-Misztal]

$A \to B$

any non-zero $a \in A$, any non-zero $b \in B$

In this 64-bit string:

0x70707070,0x07070707

one half can be 0,
the whole must be non-zero

$2^{24}-1$ differences

24 active bits

2 Rounds Further?

The most recent paper about this topic:

Martin Albrecht and Gregor Leander:

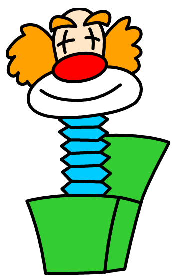
An All-In-One Approach to Differential Cryptanalysis for Small Block Ciphers, Preprint, eprint.iacr.org/2012/401.

In Section 1.1. page 3:

"*Truncated differentials, first mentioned in [15] can be seen as a collection of differentials and in some cases allow to push differential attacks one or two rounds further…* "

NOT QUITE …

⇒ For Russian GOST they allowed us to push the attack more than 20 rounds further!



8.1.3.
Better Sets [2011]

Recent Differential Attacks on GOST

References:

1. Nicolas Courtois, Michał Misztal:
Aggregated Differentials and Cryptanalysis of PP-1 and GOST,
In CECC 2011, 11th Central European Conference on Cryptology, Budapest 2011, post-proceedings in preparation.
=> invention of new sets
2. Nicolas Courtois, Michał Misztal:
First Differential Attack On Full 32-Round GOST, In ICICS'11, Beijing, China, pp. 216-227, Springer LNCS 7043, 2011.
=> first simple attack (very slightly) faster than brute force $2^{254.6}$
3. Nicolas Courtois, Michał Misztal:
Differential Cryptanalysis of GOST,
Preprint, 14 June 2011 eprint.iacr.org/2011/312.
=> progressive improved approach, heuristic and not very precise… 2^{226}
4. Nicolas Courtois:
An Improved Differential Attack on Full GOST,
Preprint Archive, 15 March 2012, eprint.iacr.org/2012/138.
=> symmetric + many further refinements + very careful work on individual bits + tight [barely working] distinguishers + justification of earlier results 2^{179}

New vs. Old Sets

- Seki-Kaneko [2000]:

  0x70707070,0x07070707

  $2^{24}-1$ differences

  24 active bits

  naturally occurs: 2^{-40}

- Courtois-Misztal [2011]

  0x80700700,0x80700700

  $2^{14}-1$ differences

  14 active bits

  naturally occurs: 2^{-50}

simultaneously bigger signal and smaller noise

New Sets [Courtois,Misztal, 2011]

NEW!

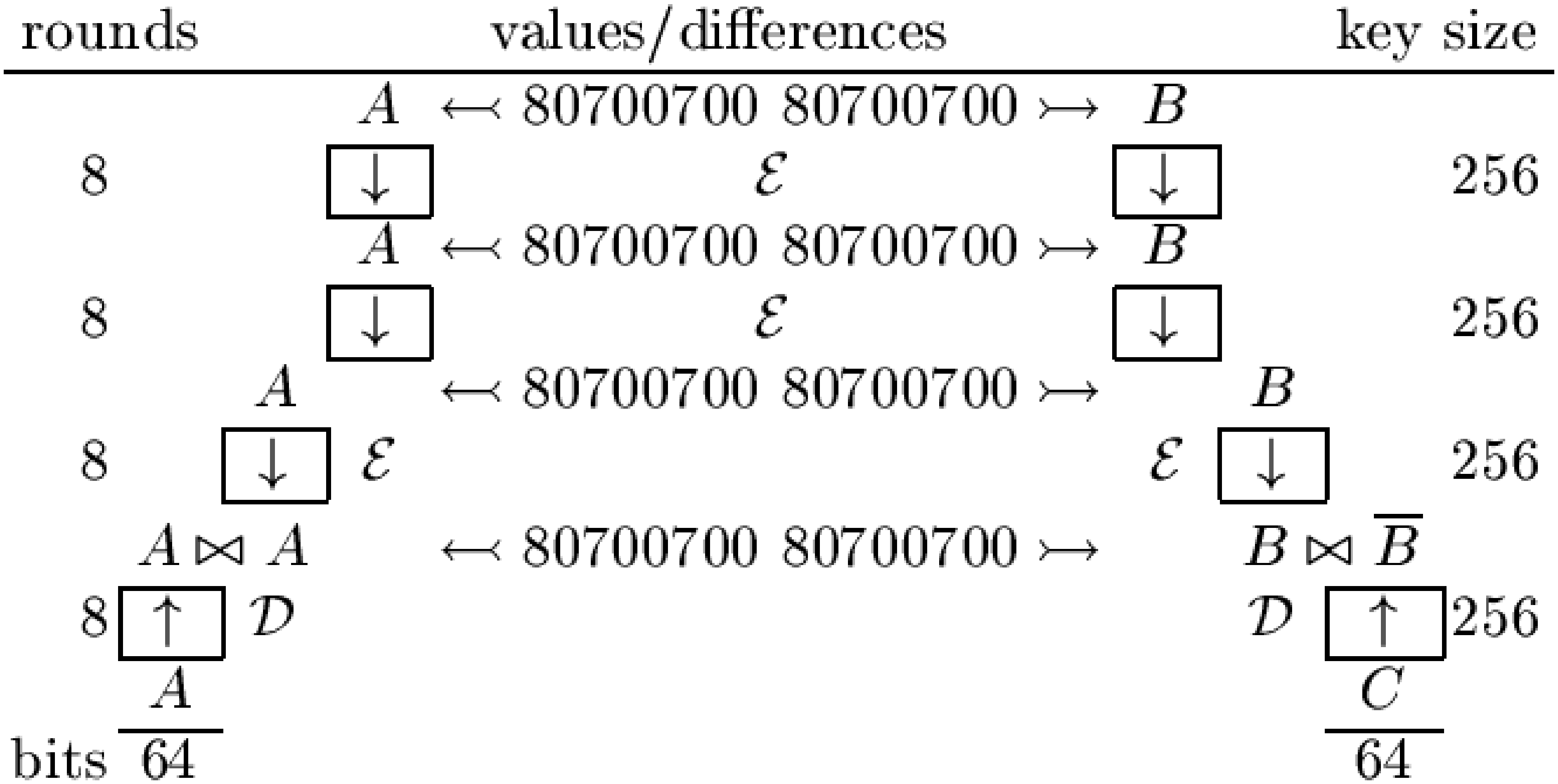
Input Aggregated Differential	0x70707070,0x07070707	0x80700700,0x80700700
Output Aggregated Differential	0x70707070,0x07070707	0x80700700,0x80700700
Reference	Seki-Kaneko [38]	this paper and [10]
Propagation 2 R	$2^{-8.6}$	$2^{-7.5}$
Propagation 4 R	$2^{-16.7}$	$2^{-13.6}$
Propagation 6 R	$2^{-24.1}$	$2^{-18.7}$
Propagation 8 R	$2^{-28.4}$	$2^{-25.0}$
Propagation 10 R	2^{-35}	$2^{-31.1}$
Propagation 12 R	2^{-43}	2^{-36}
Propagation 14 R	2^{-50}	2^{-42}
Propagation 16 R	2^{-56}	2^{-48}
Propagation 18 R	2^{-62}	2^{-54}
Propagation 20 R	2^{-70}	2^{-60}
Propagation 22 R	2^{-77}	2^{-66}
Output Δ Occurs Naturally	$2^{-40.0}$	$2^{-50.0}$

8.4.
AC Reduction+DC Attacks

NEW!

Combined DC+Algebraic Complexity Reduction

3 KP for 8R obtained. Time(8R)= 2^{110}.



UCL

9. Multiple-Point Events and Bicliqes

Attacks with Multiple Fixed Points and Bicliques

New attacks with multiple related encryptions
+ additional well-chosen properties,
as usual.

A form of advanced
higher-order differential attack.

Greatly decreases the cost of making
assumptions such as A=B' etc.

Single Key Approximate Multiple Fixed Points

=> all
8 points
share
the same
50 bits!

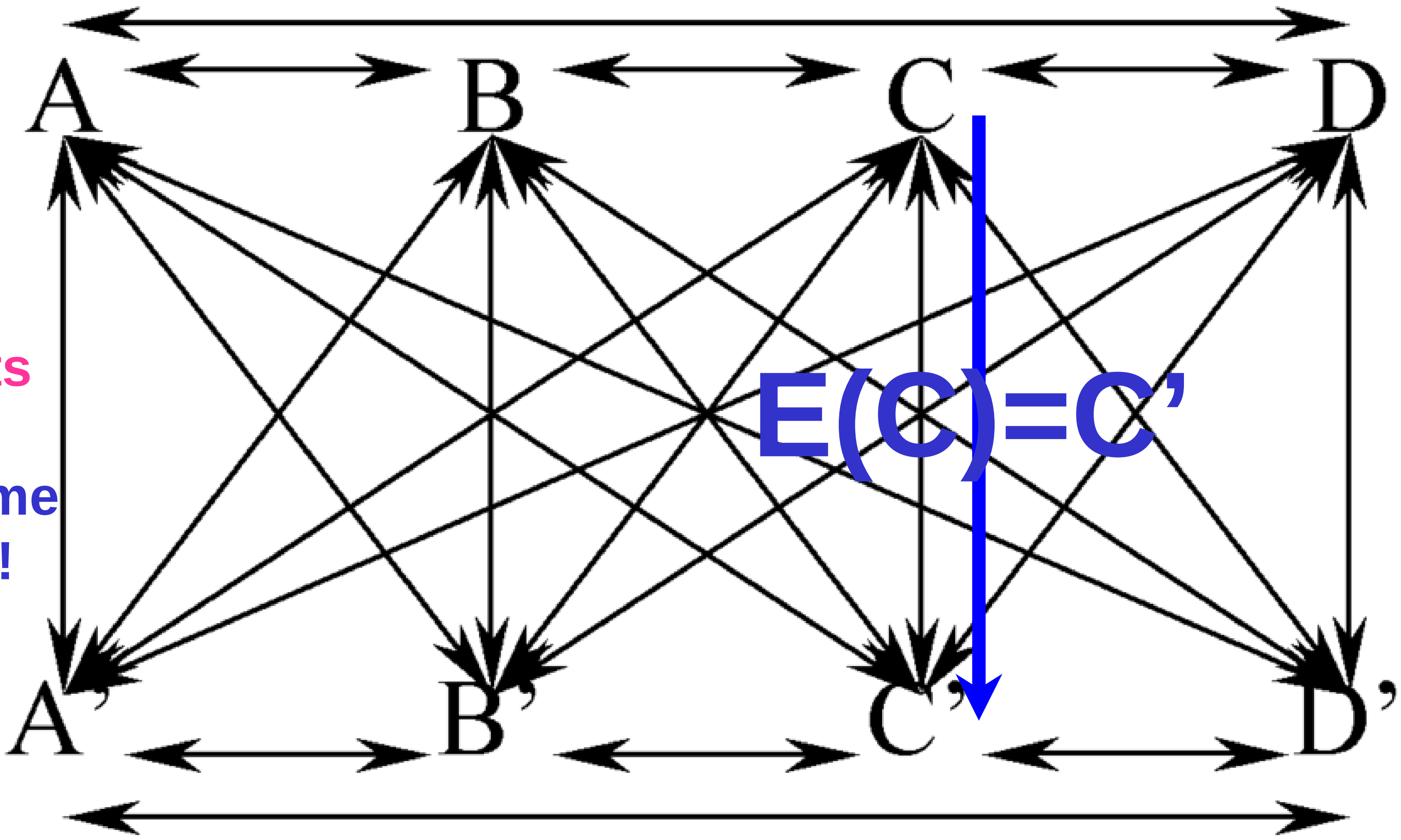


Fig. 18. An approximate fixed point biclique with $k = 4$

Attacks with Multiple Fixed Points and Bicliques

Example:

Family 8.4. Fact 73 Section 22.6.

Given 2^{79} devices with random keys on 256 bits and 2^{32} CP per key we can recover one GOST key in time of 2^{101}.

=> Nearly feasible (for a large intelligence agency).

=> Further improvements expected…

9.2.
Summary:
All Single+Multiple Key Attacks

The Multiple Key Scenario (1)

NEW!

cf. eprint.iacr.org/2011/626/

Attack Ref.	§10.3/[32]	§13.1/[32]	Red. 3 §12	[27]	F.0 [54]	Fam. 2	Fam. 2	Fam. 3	Fam. 4.X.
Keys density d	0.63		0.63	1	2^{-32}			2^{-64}	2^{-64}
Data/key 32R	2^{32} KP	2^{64} KP	2^{64} KP	2^{64} KP	2^{32} CP	2^{32} CC	2^{32} ACC	2^{64} KP	2^{32} CP/2^{64}
Obtained for 8R	**2** KP		**3** KP	-	1 KP	**3** KP	4 KP		**2** KP
Valid w. prob.	2^{-96}	2^{-64}	2^{-64}	-	2^{-1}	2^{-64}	2^{-64}	2^{-1}	2^{-0}
Storage bytes	$2^{46}/2^{39}$	$2^{46}/2^{39}$	2^{67}	2^{70}	small			2^{67}	for data
♯ False positives	2^{128}		2^{128}		2^{192}	2^{64}	2^{-0}	2^{64}	2^{128}
Time for 8 R	$2^{127}/2^{128}$	$2^{127}/2^{128}$	2^{110}	-	2^{192}	2^{110}	$\mathbf{2^{94}}$	$\mathbf{2^{94}}$	2^{128}
Attack time 32 R	$\mathbf{2^{223}}/2^{224}$	$\mathbf{2^{191}}/2^{192}$	2^{206}	$\mathbf{2^{179}}$	2^{192}	$\mathbf{2^{174}}$	$\mathbf{2^{158}}$	$\mathbf{2^{95}}$	$\mathbf{2^{128}}$
Cost of 1 key, if	$2^{224}/2^{225}$	$2^{192}/2^{193}$	2^{207}	$\mathbf{2^{179}}$	$\mathbf{2^{193}}$	2^{206}	2^{190}	$\mathbf{2^{159}}$	$\geq \mathbf{2^{129}}$
key diversity ≥	single key attacks or for > 50% of keys				2^{32}				2^{65}
Data x keys	2^{33}	2^{64}	2^{65}	2^{64}	2^{64}				2^{96} / 128

The Multiple Key Scenario (2)

NEW!

cf. eprint.iacr.org/2011/626/

Family cf.	Fam. 5.3	Fam. 5.4	Fam. 6	Fam. 7.2	Fam. 8.1	Fam. 8.2	Fam. 8.3	Fam. 8.4
Keys density d	$\mathbf{2^{-52}}$	2^{-75}	2^{-84}	2^{-84}	2^{-98}	2^{-84}	2^{-70}	2^{-79}
Data/key 32R	2^{32} ACP	2^{32} ACP	2^{33}CPCC	2^{32} ACC	2^{32} CP	2^{32} CP	2^{32} CP	2^{32} CP
Obtained for 8R	**3** KP	**4** KP	**4** KP	**6** KP	**3** KP	**3** KP	**3** KP	**4** KP
Valid w. prob.	2^{-9}	2^{-9}	2^{-0}	2^{-4}	2^{-0}	2^{-0}	2^{-0}	2^{-0}
Storage bytes	small							
♯ False positives	?	small		0	2^{64}	$> 2^{64}$	?	small
Time for 8 R	$\mathbf{2^{110}}$	$\mathbf{2^{94}}$	$\mathbf{2^{94}}$	$\mathbf{2^{83}}$	$\mathbf{2^{110}}$	$\mathbf{2^{110}}$	$\mathbf{2^{120}}$	$\mathbf{2^{94}}$
Attack time 32 R	$\mathbf{2^{119}}$	$\mathbf{2^{102}}$	$\mathbf{2^{94}}$	$\mathbf{2^{87}}$	$\mathbf{2^{110}}$	$\mathbf{2^{110}}$	$\mathbf{2^{120}}$	$\mathbf{2^{94}}$
Cost of 1 key, if	$\mathbf{2^{139}}$	$\mathbf{2^{113}}$	$\mathbf{2^{117}}$	2^{146}	$\mathbf{2^{120}}$	$\mathbf{2^{110}}$	$\mathbf{2^{120}}$	$\mathbf{2^{101}}$
key diversity $\geq$	2^{52}	2^{75}	2^{84}	2^{84}	2^{98}	2^{84}	2^{70}	2^{79}
Data x keys	2^{84}	2^{107}	2^{121}	2^{116}	2^{130}	2^{116}	2^{102}	2^{111}

Table 3. Major attacks on full GOST cipher: single vs. multiple random keys scenario. Various attacks are here compared according to their capacity to find some keys when weak keys occur at random with their natural probability. In lower table we see that if we allow higher key diversity requirements and more data collected in total (for all keys), the overall time cost to recover one key, this **including** the cost to examine keys which are not weak, decreases down to 2^{101} and beats all known single key attacks.

9.3.

Facts or Fictions?

NEW!

July 2012

In CTCrypt 2012, workshop held in English, in Russia, July 2012.

Algebraic and Differential Cryptanalysis of GOST: Fact or Fiction

https://www.tc26.ru/documentary%20materials/CTCrypt%202012/slides/CTCrypt_rudskoy_slides_final.pdf

A. Dmukh, V. Rudskoy

→ 8R algebraic attack is not well-grounded

~~Fact~~ Fiction 3 (Key Recovery for 4 Rounds and 2 KP)

Easy: try CryptoMiniSat

~~Fact~~ Fiction 5 (Key Recovery for 8 Rounds and 3 KP)

See Cryptologia Jan 2013 and eprint/2011/626

→ Differential attacks

- S-boxes heavily affect security
- With "good" S-boxes the attack fails

Super naïve: it makes little sense to take our differential property optimised for one set of S-boxes and apply it to another set of S-boxes.
Another differential property is needed; carefully optimised for this another set of S-boxes…

UCL

11. Diffusion in GOST

Guess-Then-Determine

UNSAT Immunity

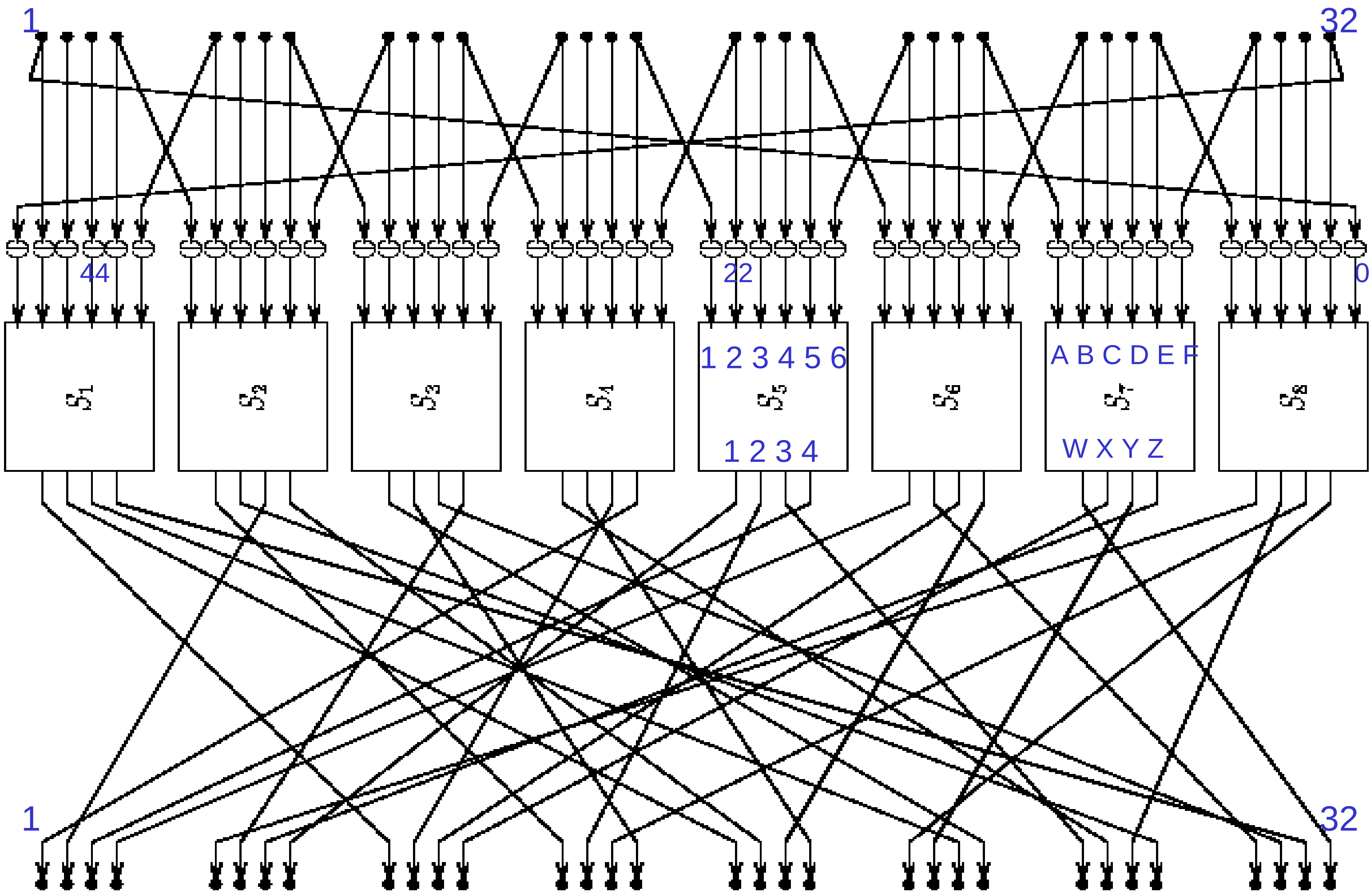
*Claims on GOST

Wikipedia April 2011:

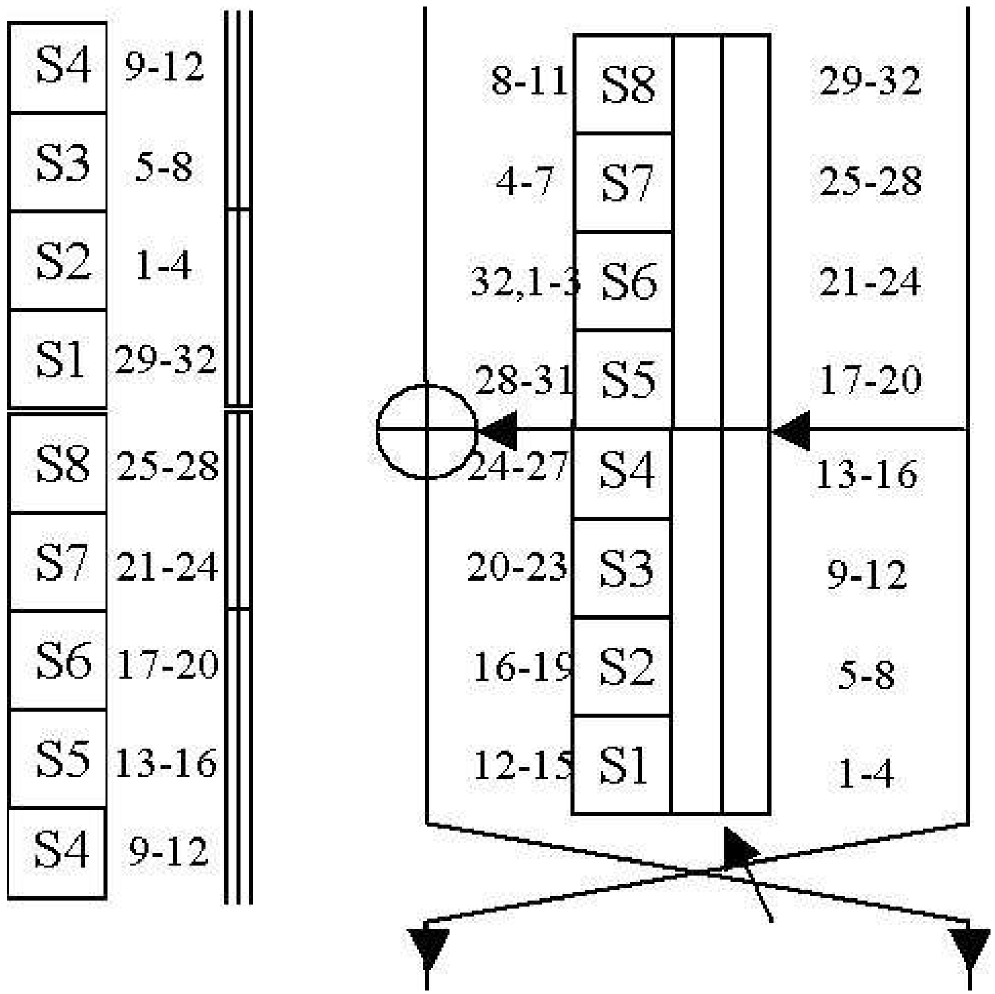
Cryptanalysis of GOST

…Another concern is that the avalanche effect is slower to occur in GOST than in DES. This is because of GOST's lack of an expansion permutation in the round function, as well as its use of a rotation instead of a permutation. Again, this is offset by GOST's increased number of rounds…

DES:



1 Round + Next Round of GOST



Carry Propagation

determine a:

need S3, S4 and c

3 1 1

d,e known

=> $2^{0.6}$ possibilities

↓

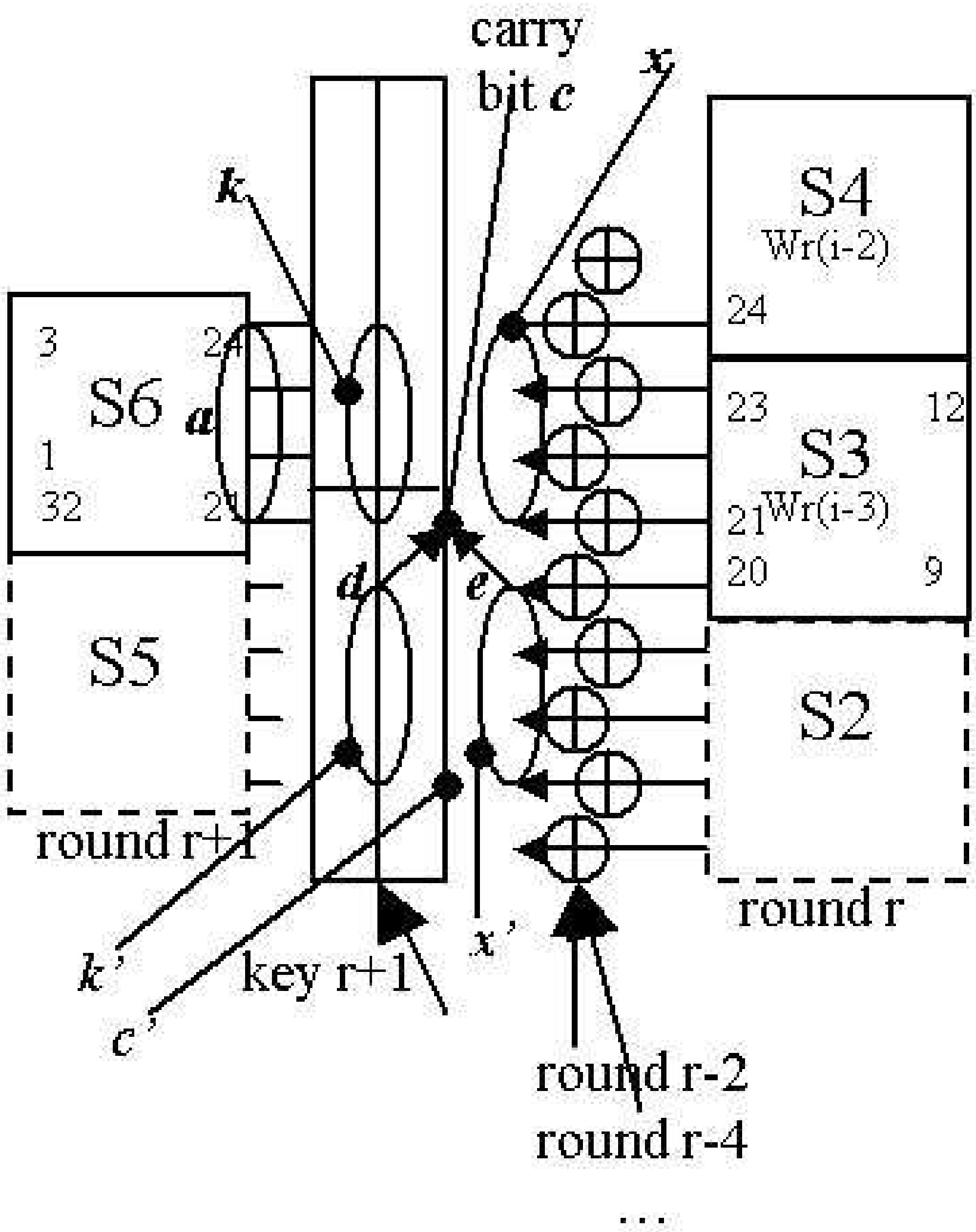
3 more bits known

=> $2^{0.3}$ possibilities

↓

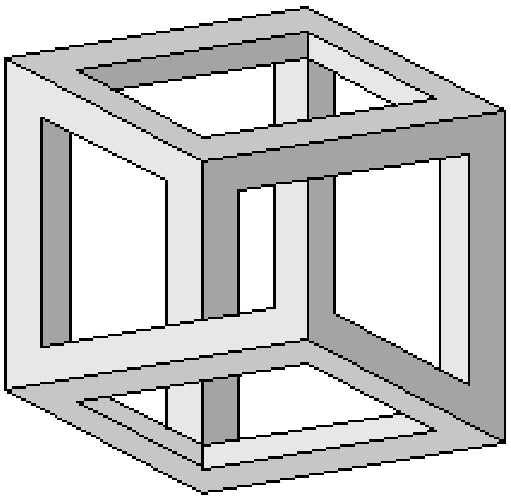
…

$2^{0.0}$



11.2. Guess-Then-Determine:
What to Guess?

11.2.1.
Contradiction Immunity



Attacks With SAT Solvers

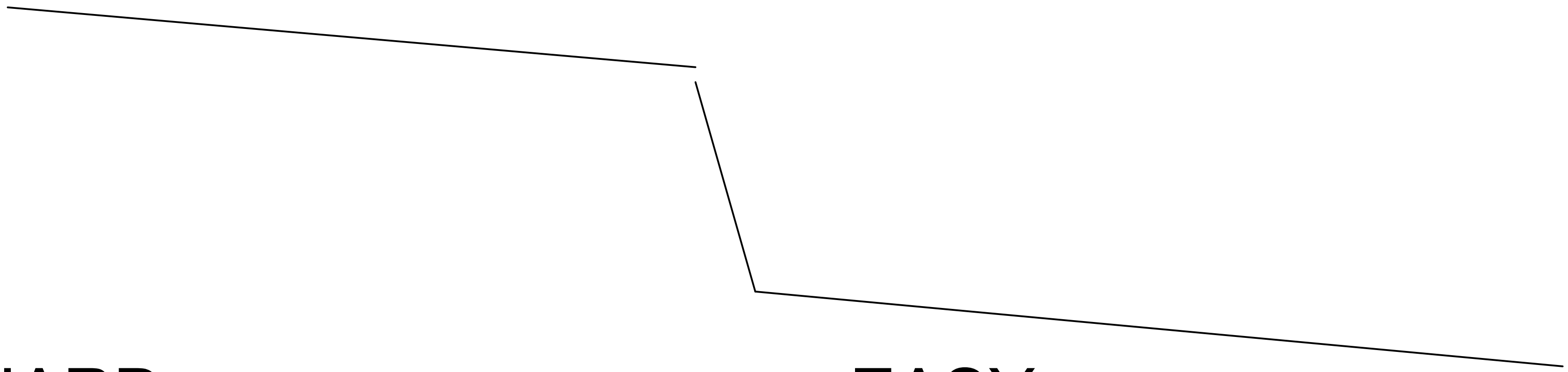
2 strategies:

There are two main approaches in SAT cryptanalysis or two main algorithms to break a cipher with a SAT solver:

1. **The SAT Method:** Guess X bits and run a SAT solver which, if the assumption on X bits is correct takes time T. Abort all the other computations at time T. The total time complexity is about $2^X \cdot T$.
2. **The UNSAT Method:** Guess X bits and run a SAT solver which, if the assumption on X bits is incorrect finds a contradiction in time T with large probability $1 - P$ say 99 %.
   With a small probability of $P > 0$, we can guess more key bits and either find additional contradictions or find the solution.
   The idea is that if P is small enough the complexity of these additional steps can be less then the $2^X \cdot T$ spent in the initial UNSAT step.
3. **A Mixed UNSAT/SAT Attack:** In practice maybe P is not as small as we wish, and therefore we may have a mix of SAT and UNSAT method: where the final complexity will be a sum of two terms none of which can be neglected. We will see some specific examples later.

Phase Transitions for Naïve Cryptologists:

1 dimensional



HARD ……………………….. EASY

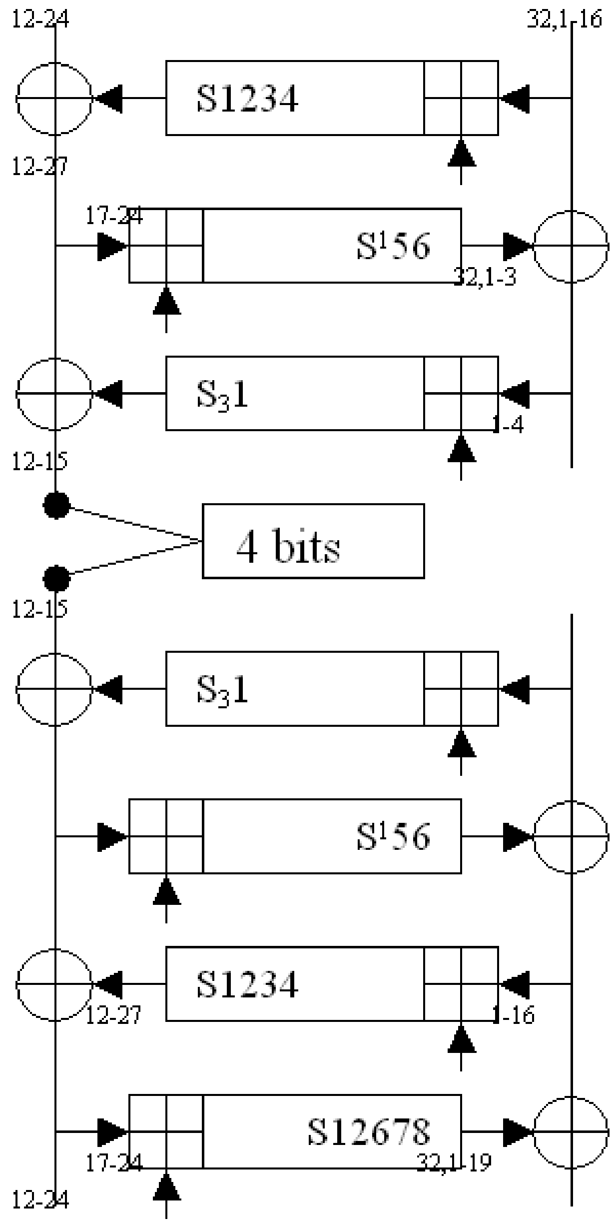
For Serious Cryptologists:

In fact we need to look
at an exponential number of subsets!

UNSAT Immunity

Well chosen set of 68 bits.

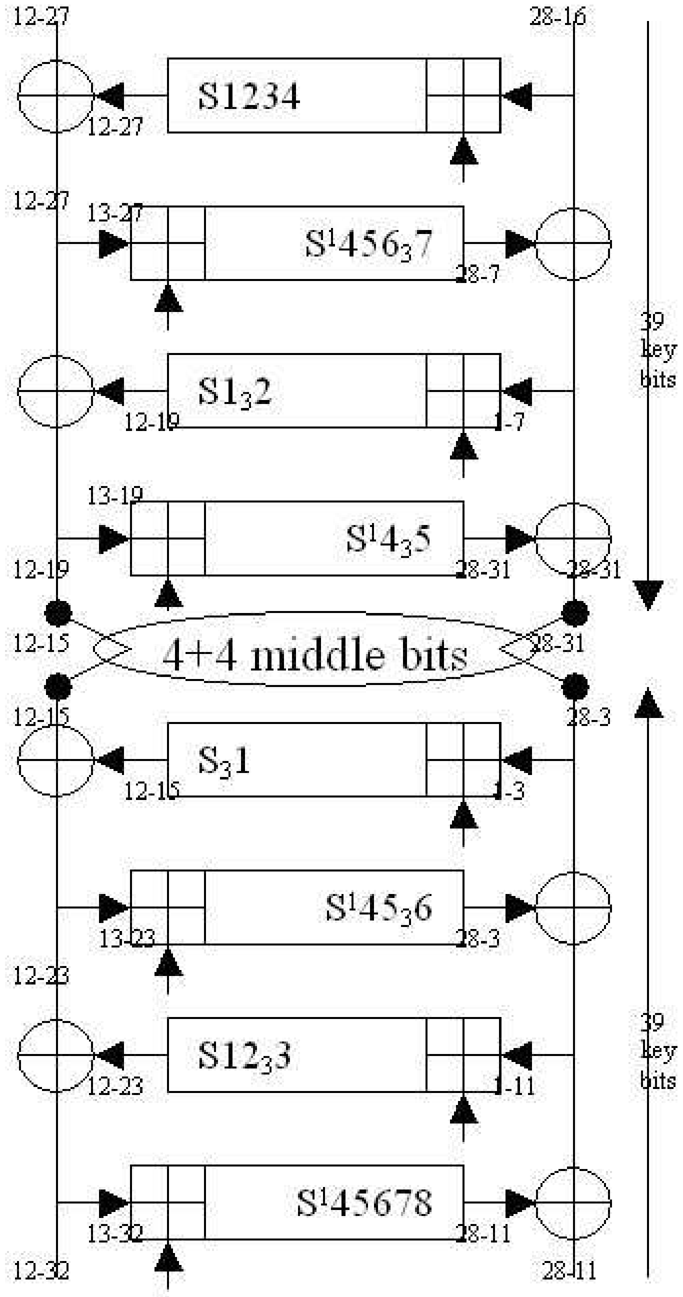
UNSAT proba=39%.



Jumps…

To increase 39% to 50%
we need 10 more bits
= 78 bits.

UNSAT proba=50%.



UNSAT Immunity in DES

Fact 1. The Contradiction Immunity is at most 44 for 8 rounds of DES.

For 8 rounds of GOST:

it is 78 [unpublished set].

More on UNSAT Immunity

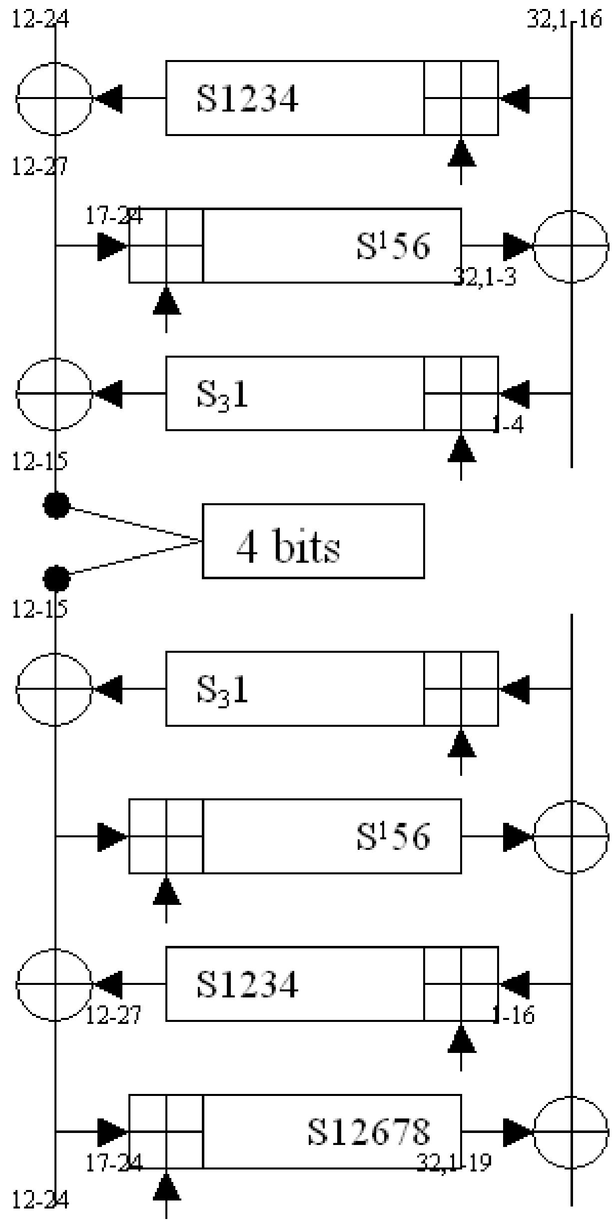
See:

Nicolas Courtois, Jerzy A. Gawinecki, Guangyan Song: Contradiction Immunity and Guess-Then-Determine Attacks On GOST,
In Tatra Mountains Mathematic Publications,
53 (2013), pp. 1-15?

SAT Immunity – 4 pairs

Same set of 68 bits as before.

=> all the other bits?

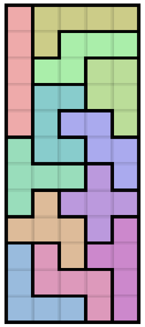


SAT Immunity – 4 pairs

Same set of 68 bits as before.

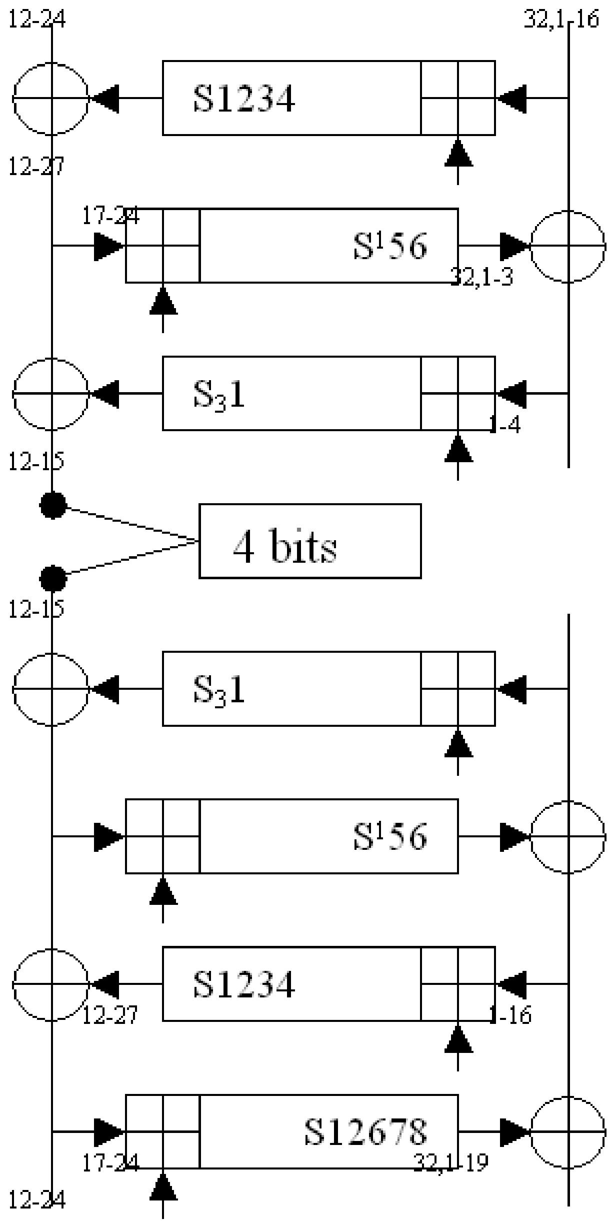
=> all the other bits are found in 400 s on one laptop i7 CPU

⇒ using CryptoMiniSat x64 2.92.

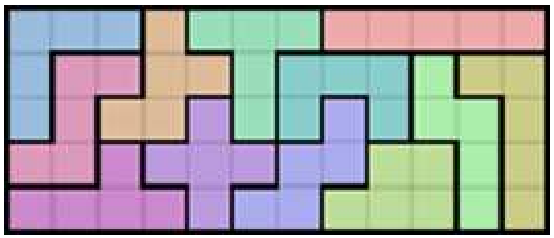


Corollary: Given 4KP for 8R we determine all the key bits in time 2^{94}.

[Courtois Cryptologia vol 37, 2013]

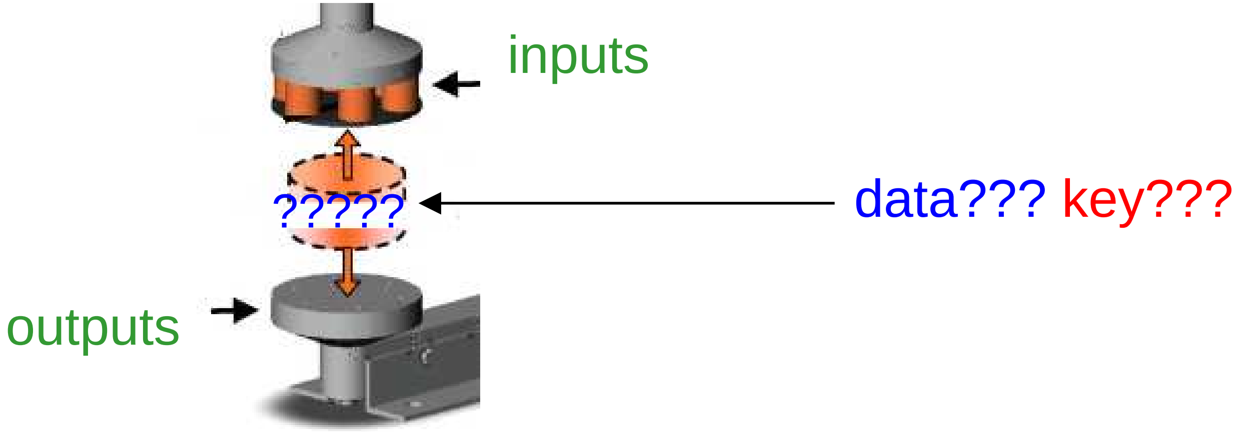


*12. Another take on it: Inference, Induction, Saturation Analysis

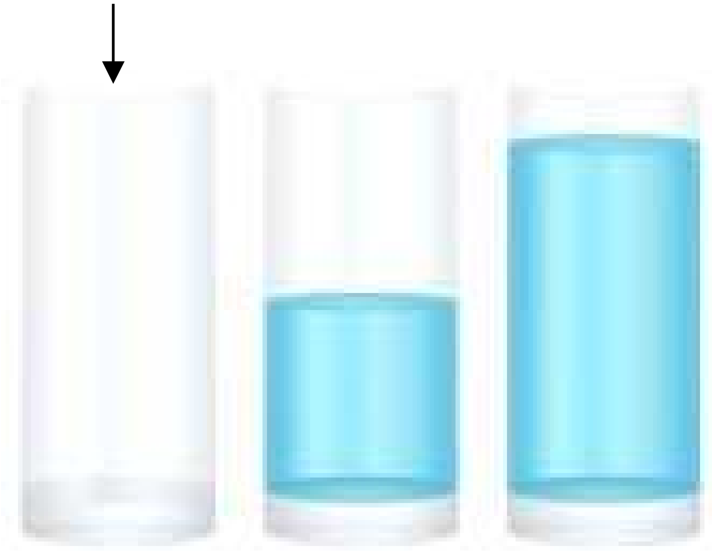


or how “order” emerges in various attacks

Overcoming Chaos



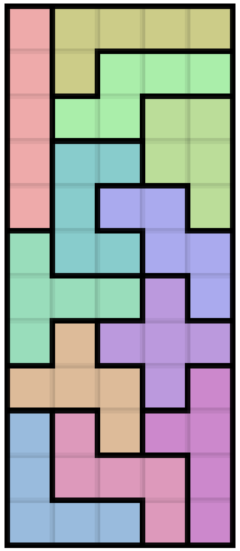
Add Information => Amplify => Solve



more constraints => saturation?

Growth Leads To Saturation

=> …. =>



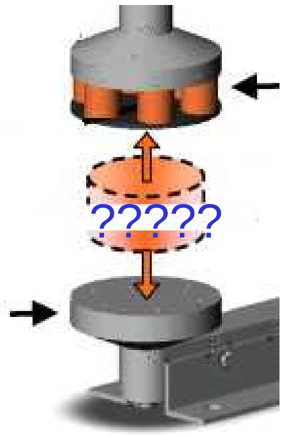
Add Info => Emerging Order => Inference

Amplification Saturation

2x determine all

phase transition
hard=>easy

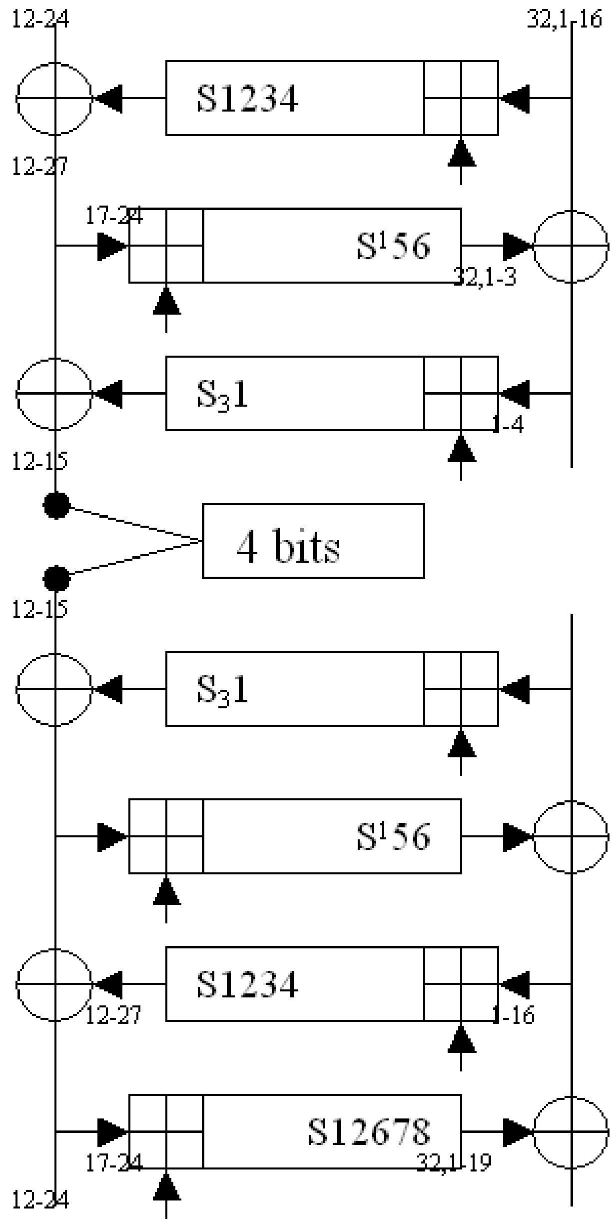
12.1.
SAT Immunity
≥1KP



SAT Immunity – 4 pairs

Same set of 68 bits as before.

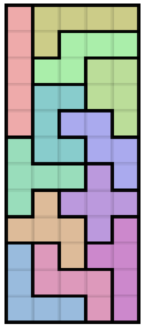
=> all the other bits?



SAT Immunity – 4 pairs

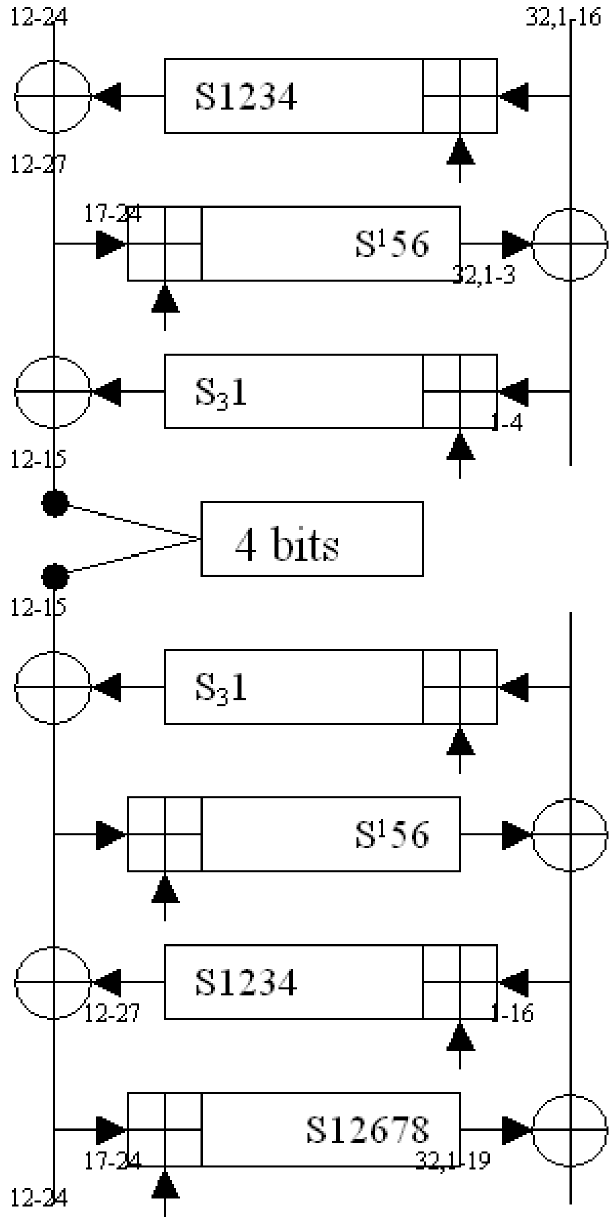
Same set of 68 bits as before.

=> all the other bits
are found in 400 s on
one laptop i7 CPU
⇒ using CryptoMiniSat x64 2.92.



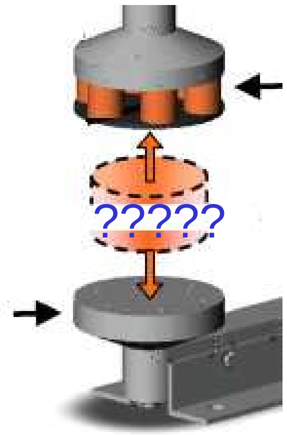
Corollary: Given 4KP for 8R
we determine all the key bits
in time 2^{94}.

[Courtois Cryptologia vol 37, 2013]



12.2.
Inference With 1KP

yes, due to the key schedule



First 16 Rounds of GOST

1 point, first 16 rounds of GOST

A		A
		(8 Rounds)
(16 Rounds)	becomes	A
	$P \approx 50\ \%$	(8 Rounds)
A		A
1 bit		65 bits

A is an arbitrary unknown value

Fig. 29. Fixed points in the first 16 rounds of GOST seen as an Induction property: the value in the middle is obtained nearly for free instead of 2^{-64}

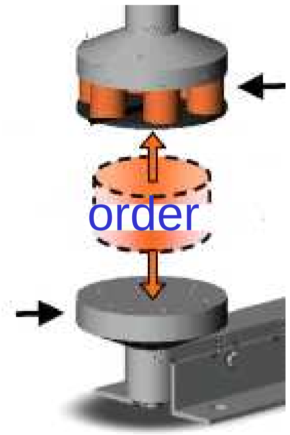
Compare to Last 16 Rounds:

1 point, LAST 16 rounds of GOST

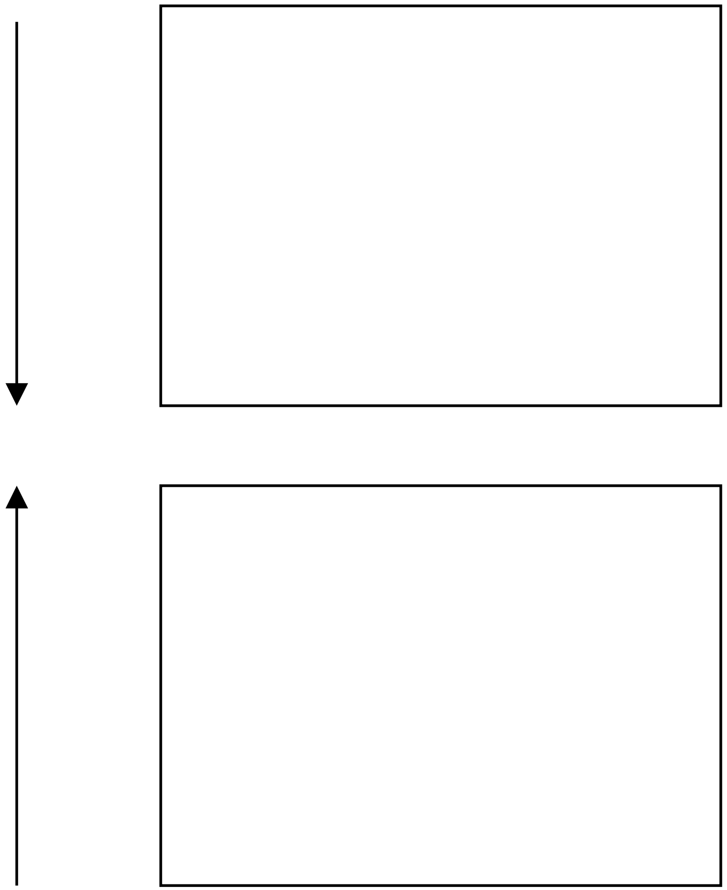
A		A
		(8 Rounds)
(16 Rounds)	becomes	symmetric
	100 %	(8 Rounds)
A		A
0 bit		32 bits

A is an arbitrary unknown value, many solutions

12.3.
Differential Induction:
2, 3, 4 KP



Differential Induction = Two-Sided Propagation



Any 16 Rounds of GOST

```
2 points
        A,B sharing 50 bits                          A,B sharing 50 bits
       0x80700700 0x80700700                       0x80700700 0x80700700
                                                        (8 Rounds)
            (16 Rounds)            becomes         0x80700700 0x80700700
                                                        (8 Rounds)
       0x80700700 0x80700700                       0x80700700 0x80700700
        C,D sharing 50 bits                          C,D sharing 50 bits

            50+50 bits                                  150 bits
            2^28 events                                 2^27 events
```

50 %

Fig. 31. Differential Induction: 50 additional differences nearly for free instead of 2^{-50}

20 Rounds

2 points

A,B sharing 63 bits		A,B sharing 63 bits
0x80000000 0x00000000		0x80000000 0x00000000
		(10 Rounds)
(20 Rounds)	becomes	0x80700700 0x80700700
	50 %	(10 Rounds)
0x00000000 0x80000000		0x00000000 0x80000000
C,D sharing 63 bits		C,D sharing 63 bits
128 bits		178 bits
2^-1 events		2^-2 events

more rounds requires stronger I/O constraints

3 Points

3 points

A,B,C sharing 50 bits
0x80700700 0x80700700

(16 Rounds)

0x80700700 0x80700700
D,E,F sharing 50 bits

200 bits
2^-3+2^-11 events

becomes
99.5 %

A,B,C sharing 50 bits
0x80700700 0x80700700
(8 Rounds)
0x80700700 0x80700700
(8 Rounds)
0x80700700 0x80700700
D,E,F sharing 50 bits

300 bits
2^-3 events

3 points make it quite strong