On Optimal Size in Truncated Differential Attacks

Nicolas Courtois[1], Theodosis Mourouzis[1], Anna Grocholewska-Czurylo[2] and Jean-Jacques Quisquater[3]

[1] University College London, UK
[2] Poznań University of Technology, Poland
[3] UCL, Louvain La Neuve, Belgium

Motivation

CECC 2011 in Debrecen:

Nicolas T. Courtois, Michal Misztal: **Aggregated differentials and cryptanalysis of PP-1 and gost.** Periodica Mathematica Hungarica 65(2): 177-192 (2012)

Central European Conference on Cryptology 2013

26—28. June, 2013, Telč, Czech Republic

Position VIII: Anna Grocholewska-Czurylo.

Cryptographic Randomness Testing of Block Ciphers and Hash Functions

eprint.iacr.org/2010/564

Ali Doğanaksoy, Barış Ege, Onur Koçak and Fatih Sulak

History of DC

New paper to appear soon:

Nicolas T. Courtois, Theodosis Mourouzis, Michal Misztal, Jean-Jacques Quisquater, Guangyan Song: Can GOST Be Made Secure Against Differential Cryptanalysis?, accepted to Cryptologia, to appear in 2014.

History of DC

Differential Cryptanalysis (DC)

- based on tracking of changes in the differences between two messages as they pass through the consecutive rounds of encryption.
- one of the oldest classical attacks on modern block ciphers, if not the oldest.
- ALL ciphers should resist it…

History of DC

Coppersmith [IBM DES design team] have reported that this attack was already known to IBM designers around 1974.

It was known under the name of T-attack or Tickle attack.

It appears that

- DES have already been designed to resist to this type of attack
- IBM have agreed with the NSA that the design criteria of DES should not be made public. This precisely because it would
  “weaken the competitive advantage
  the United States enjoyed over other countries
  in the field of cryptography”

Our Research

We dispute the idea that DC is well understood.

It isn't.

We found some mistaken claims in the literature:

- Mild misunderstandings about which attacks are "the best" and what the comparison metric is..
- Cosmic misunderstandings about which ciphers are secure against DC… and how many rounds can be broken.
- Unexplored combinatorial complexity.

GOST vs. 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.

Cf. Nicolas Courtois: An Improved Differential Attack on Full GOST, preprint Archive, 15 March 2012, eprint.iacr.org/2012/138. 32 rounds, 2^{179}

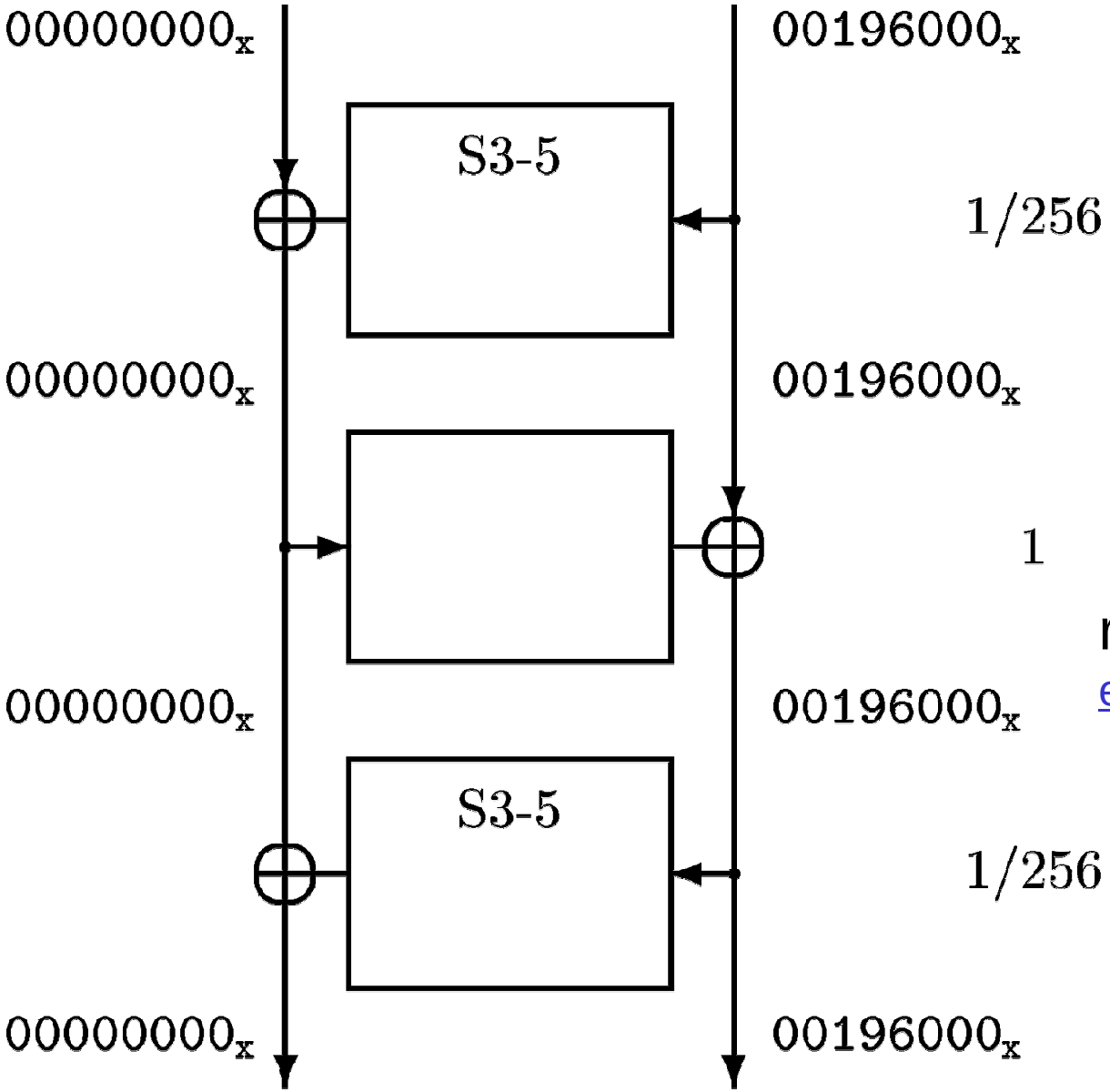


Figure 1: An example of Differential Cryptanalysis

DC on DES [Biham-Shamir]

revisited:
eprint.iacr.org/2005/202

DC Complexity

Simple “naïve” attack like Biham-Shamir attack on DES.

Assume “Differential Property of any kind”

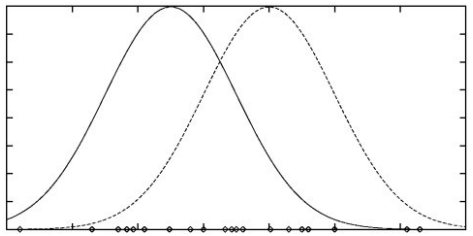
Propagation $P = 2^{-X}$

This Assuming there is no “noise”.

Guess some key bits => observe an “exceptional” event

=> right key with high proba.

Advanced differential attacks: “signal” + “noise”.



Use Gauss error function.

Biham-Shamir DC and GOST

If our model was DES…

we have totally misunderstood differential cryptanalysis.

Gabidulin 2000-2001:

Also claimed that 7 rounds are sufficient

to protect GOST against DC.

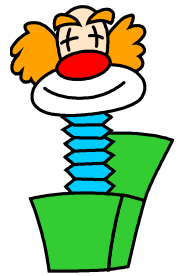
How To Be Led Astray

There are many papers about “provably security of ciphers” against DC and LC. Such works was published also about GOST, even in 2010…

⇒ In fact it is possible to CHEAT someone and to make them believe that GOST is provably secure against DC…

⇒ While in reality GOST in insecure against DC!

How interesting…



2 Rounds Further?

The most recent paper about this topic:

Martin Albrecht and Gregor Leander:

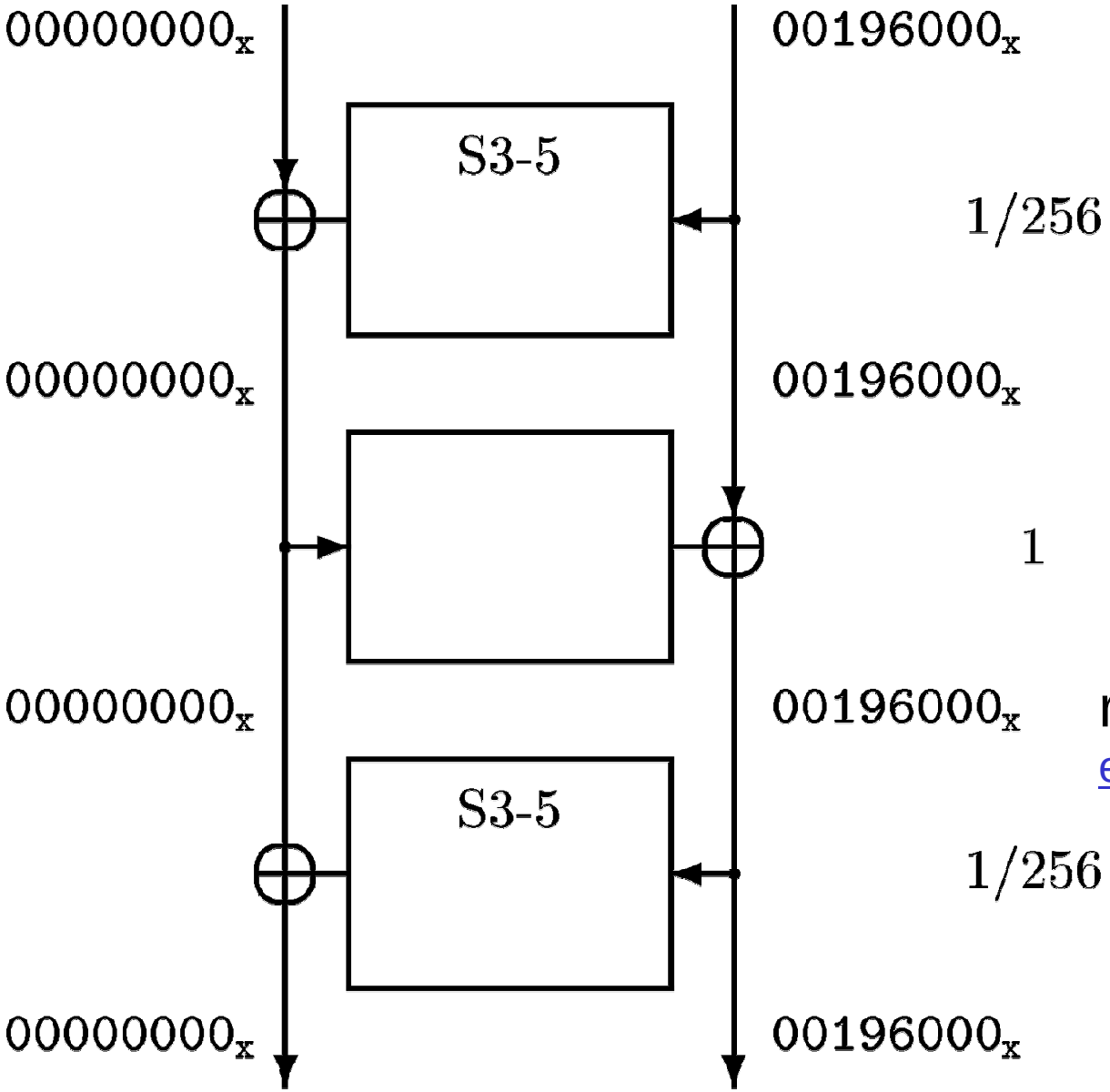
An All-In-One Approach to Differential Cryptanalysis for Small Block Ciphers, Preprint, eprint.iacr.org/2012/401.

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!



DES:

Quasi constant probability, or 2 cases…

revisited:
eprint.iacr.org/2005/202

Figure 1: An example of Differential Cryptanalysis

GOST vs. DES

DES: quasi constant probability. Does not become zero typically.

GOST, general case: propagation probability depends on the key.
Can be zero.

The problem:

For some keys it will be 0.
With probabilities as high as ½ or similar.

If for some keys it is 0,

then however strong it can sometimes be…
it is guaranteed to be 0 after a few rounds(!)

(assuming independent round keys…)

Our early estimation: a single differential attack on GOST would propagate with probability not better than 2^{-62} for 32 rounds.

For most keys it would propagate with probability 0.

14.
Advanced DC

14.1.
DC With Sets
Truncated Properties
Combinatorial Exploration

More Differential Cryptanalysis

[Seki, Kaneko SAC 2000]:

Sets of differentials = most general

Incomplete/truncated Differentials = With free bits…

Between 12 and 17 rounds out of 32 can be broken…

No attack beyond.

Or it is not clear how one would proceed: signal>noise…

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

$$A \rightarrow B$$

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

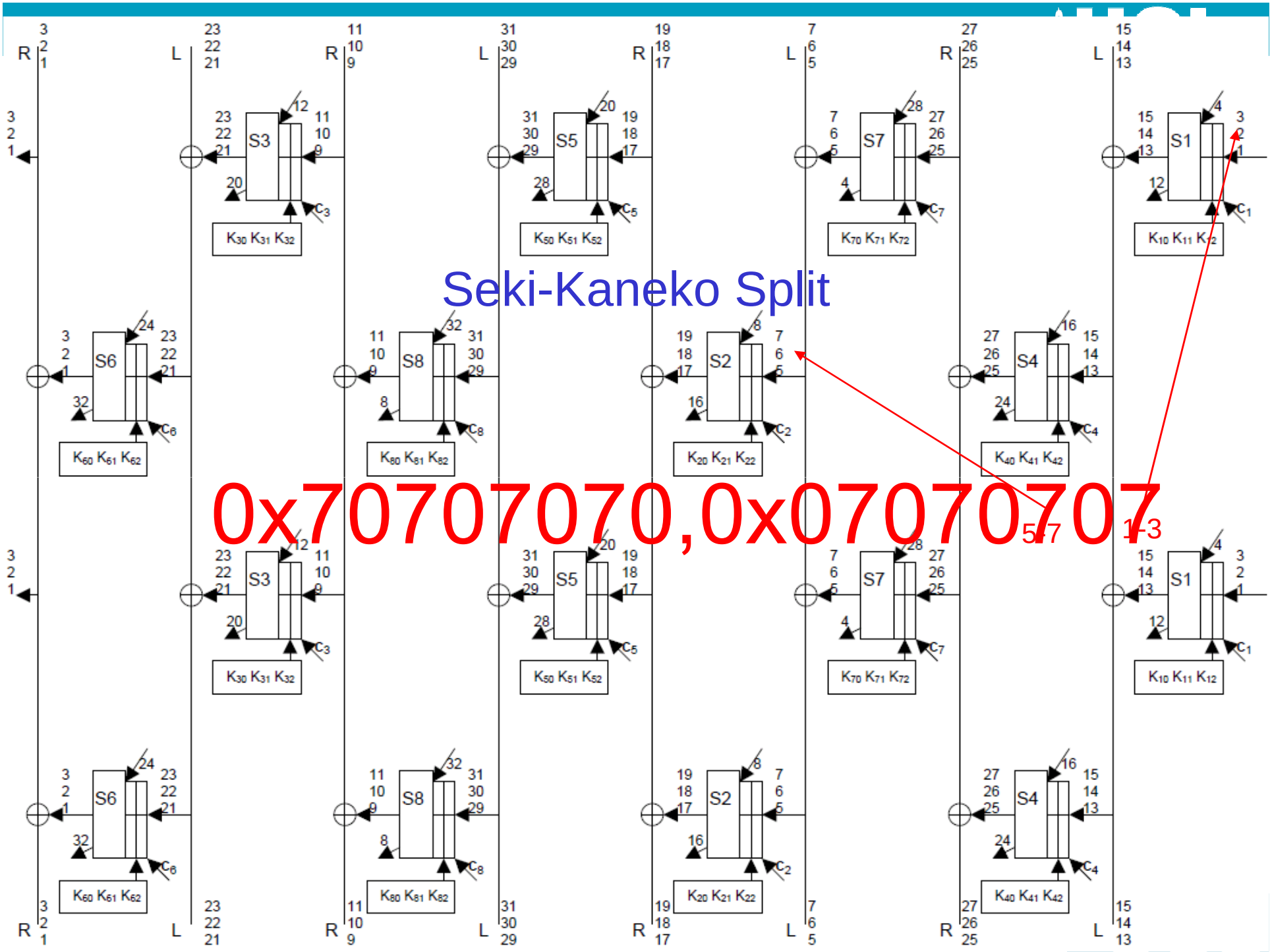
In this 64-bit string:

0x70707070,0x07070707

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

$2^{24}-1$ differences

24 active bits


Seki-Kaneko Split
0x70707070,0x07070707
S1
S2
S3
S4
S5
S6
S7
S8
K10 K11 K12
K20 K21 K22
K30 K31 K32
K40 K41 K42
K50 K51 K52
K60 K61 K62
K70 K71 K72
K80 K81 K82
R
L

Seki-Kaneko Set

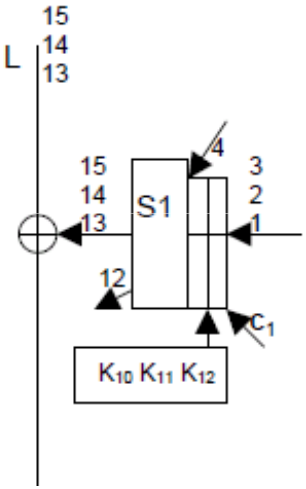
3 bits active per every second box.

S1357 in odd rounds 1,3,…

S2468 in even rounds 2,4,…

Rough estimation: there are only 4 bits coming “out” in each round. These differences must be 0 “by accident”.

Maybe 0x70707070,0x07070707 propagates with probability 2^{-4} per round?

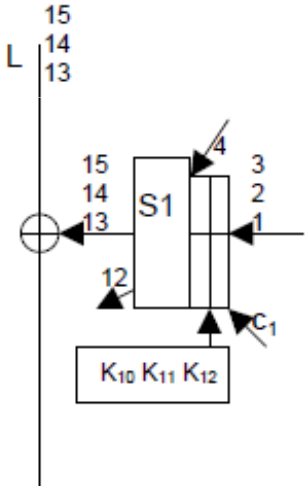


Seki-Kaneko Set (contd.)

4 bits coming “out” in each round.
these differences must be 0 “by accident”.

So 0x70707070,0x07070707 propagates with probability 2^{-4} per round?

Not quite. There are also carries: on picture bits 123 active, 4 always inactive, S2 will be active with proba about
$1-3.5/16 = 2^{-0.36}$.



So we expect $2^{-4-3.5*0.36} = 2^{-5.3}$.

Simulations also give $2^{-5.3}$ average

(odd vs. even rounds, for the S-boxes of Central Bank of Russia)

Seki-Kaneko

Is 0x70707070,0x07070707 dangerous?

Probability $2^{-5.3}$ for 1 round.

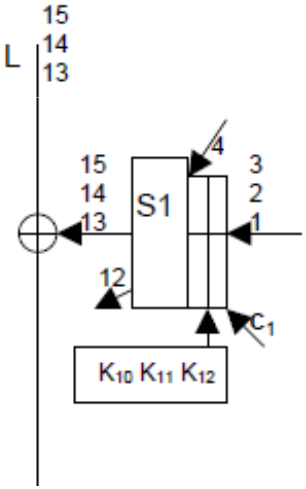
Means 2^{-170} for 32 rounds.

No hope to break GOST so far.

There is only $2^{64+24-1} = 2^{87}$

pairs with input difference

$\in$ 0x70707070,0x07070707.



Very Surprising

Propagation is MUCH better than expected. Already true for this old Japanese set from 2000.

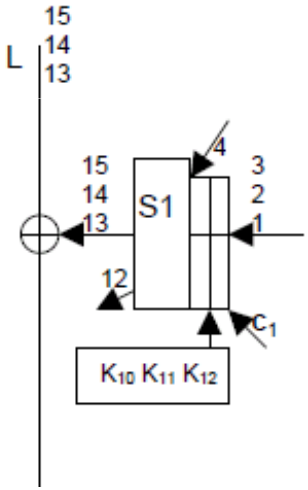
0x70707070,0x07070707.

Strong improvement. Examples:

2 Rounds: predicted $2^{-10.6}$ actual $2^{-8.6}$.

4 Rounds: predicted $2^{-21.2}$ actual $2^{-16.7}$.

8 Rounds: predicted $2^{-42.4}$ actual $2^{-28.4}$.



14.2.
Better Sets [2011]

New Sets [Courtois-Misztal, 2011]

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

New vs. Old Sets

- Seki-Kaneko:

0x70707070,0x07070707

$2^{24}-1$ differences

24 active bits

naturally occurs: 2^{-40}

- Courtois-Misztal

0x80700700,0x80700700

$2^{14}-1$ differences

14 active bits

naturally occurs: 2^{-50}

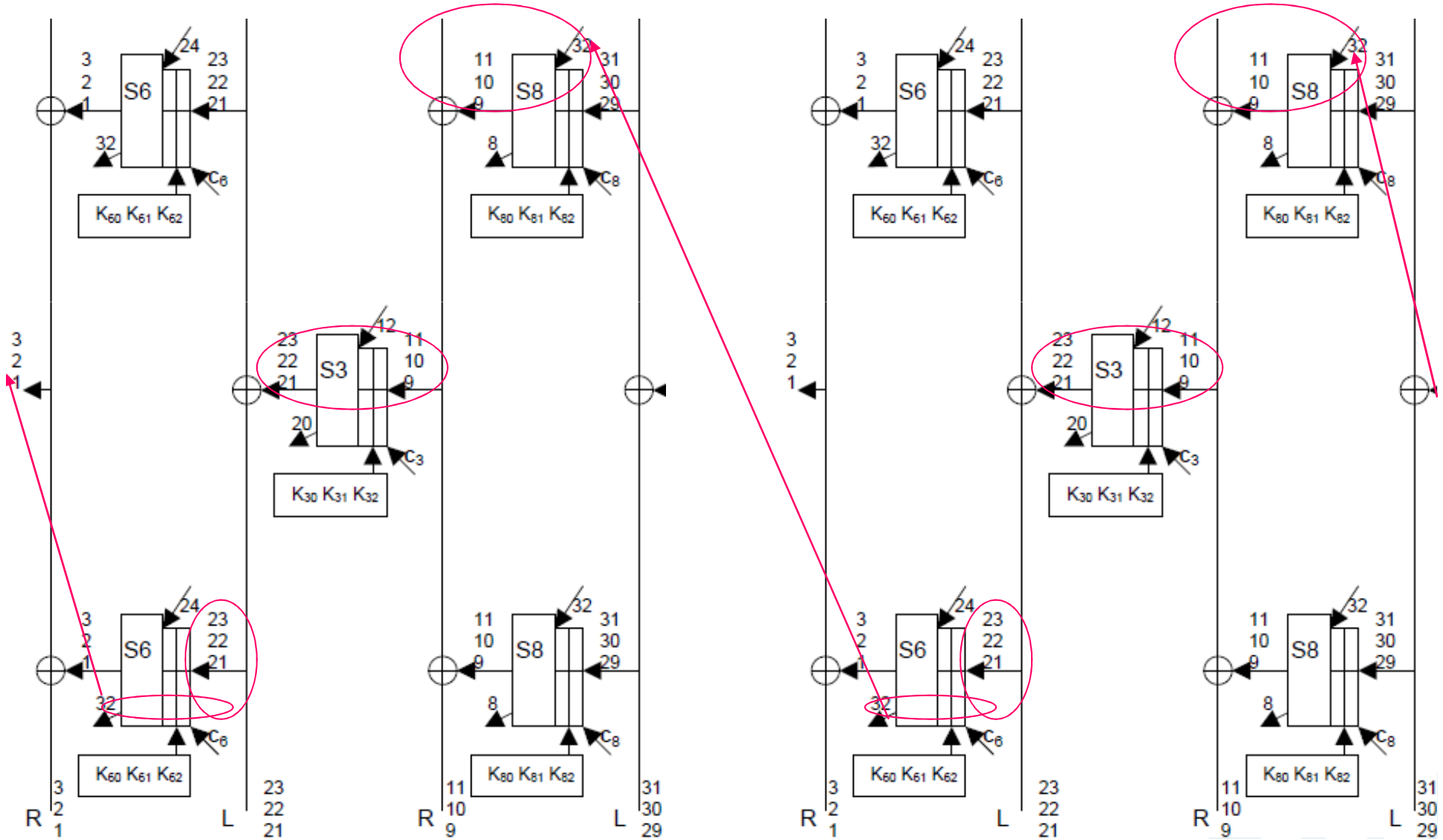
simultaneously bigger signal and smaller noise

New Sets [Courtois,Misztal, 2011]

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	$2^{-40.0}$	$2^{-50.0}$

0x80700700,0x80700700

Type 3+3: S836 + S836



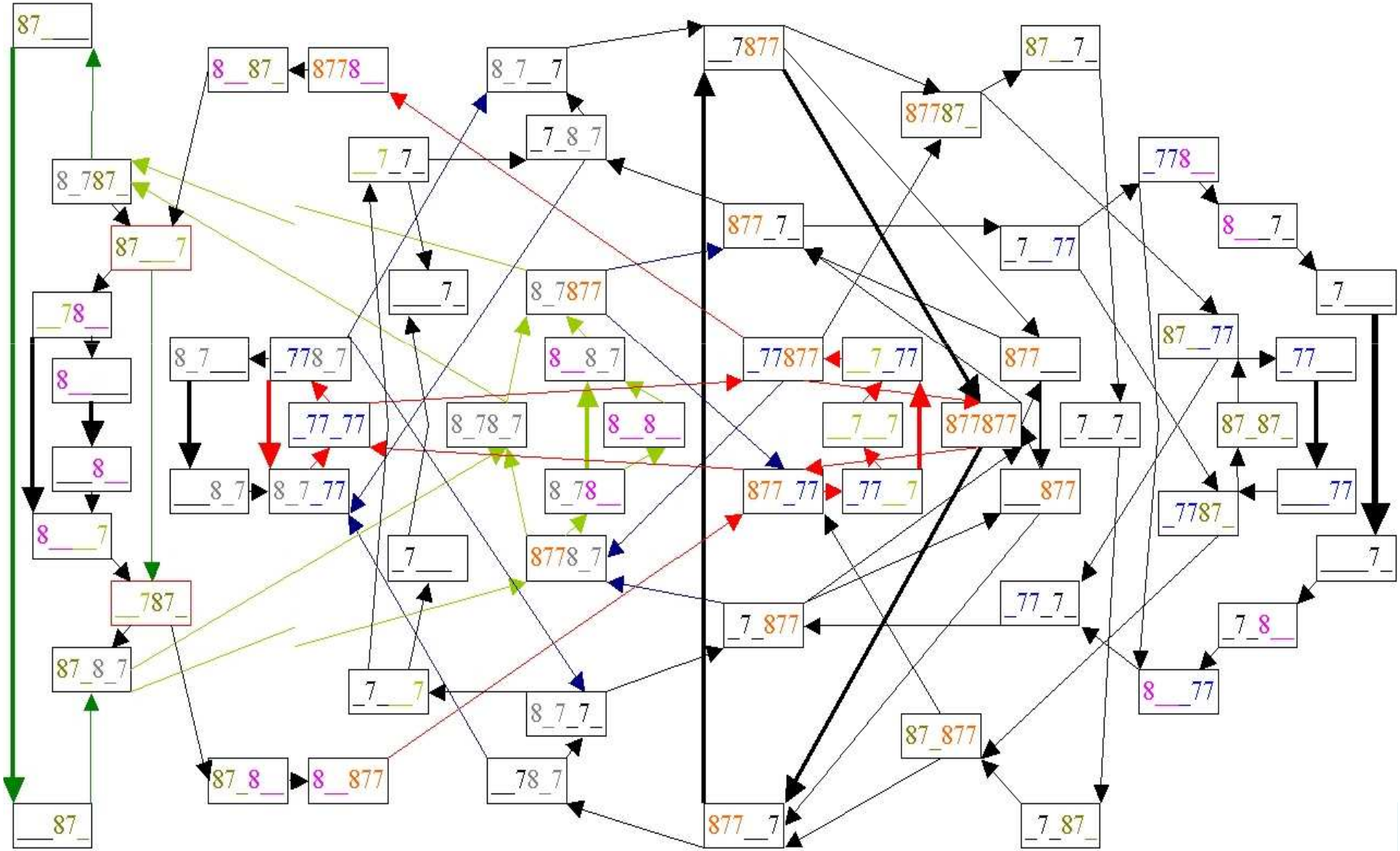
14.3.
Truncated Diff. Propagation

How To Find Such An Attack

Best differential property
we ever found was found BY HAND.

Is a systematic approach possible?

Our Attack = Graph Walks With Costs



Propagation – 7R

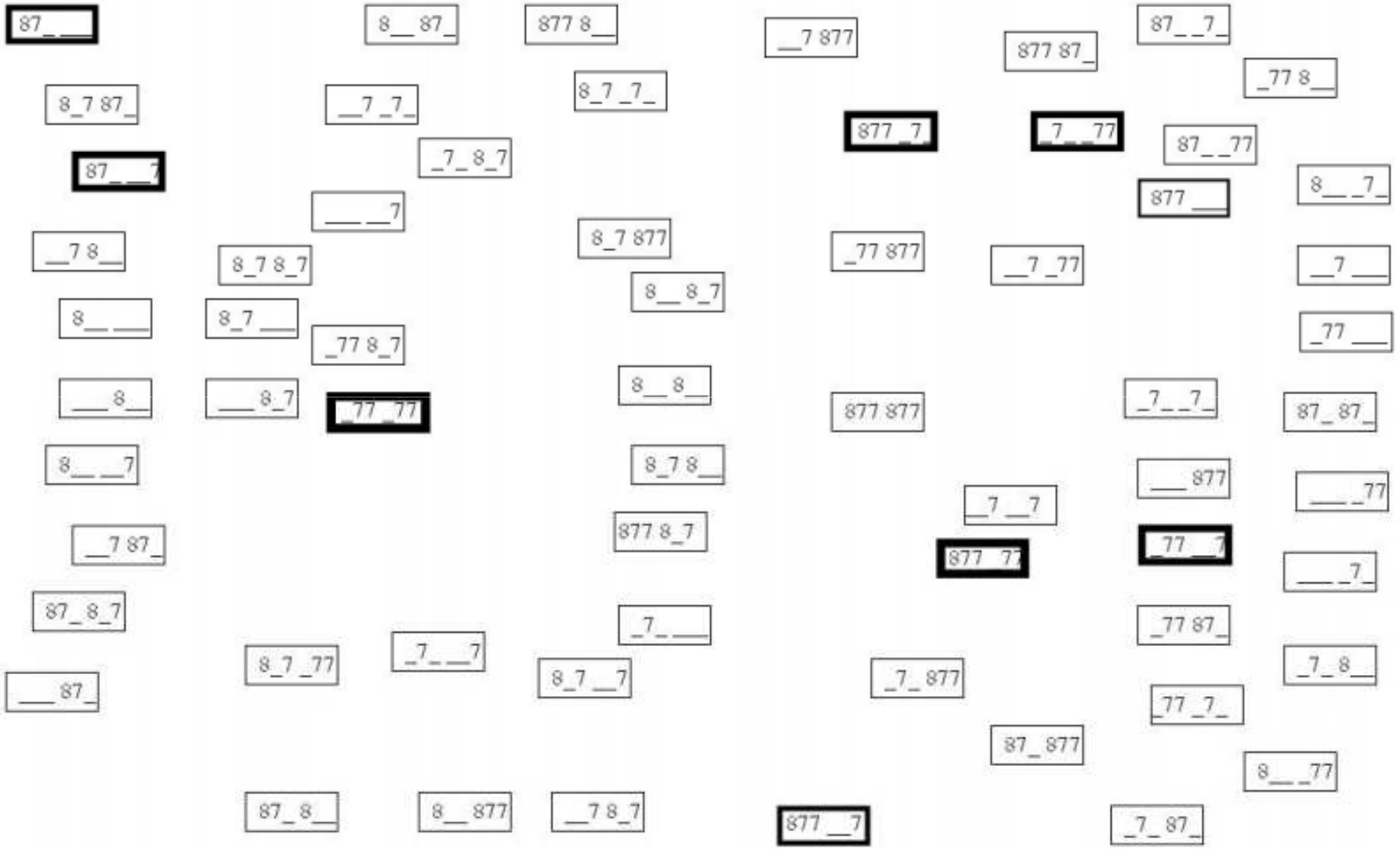


Figure 3: Propagation of (80000000, 00000000) after 7R

and 8R – still concentrates at few places

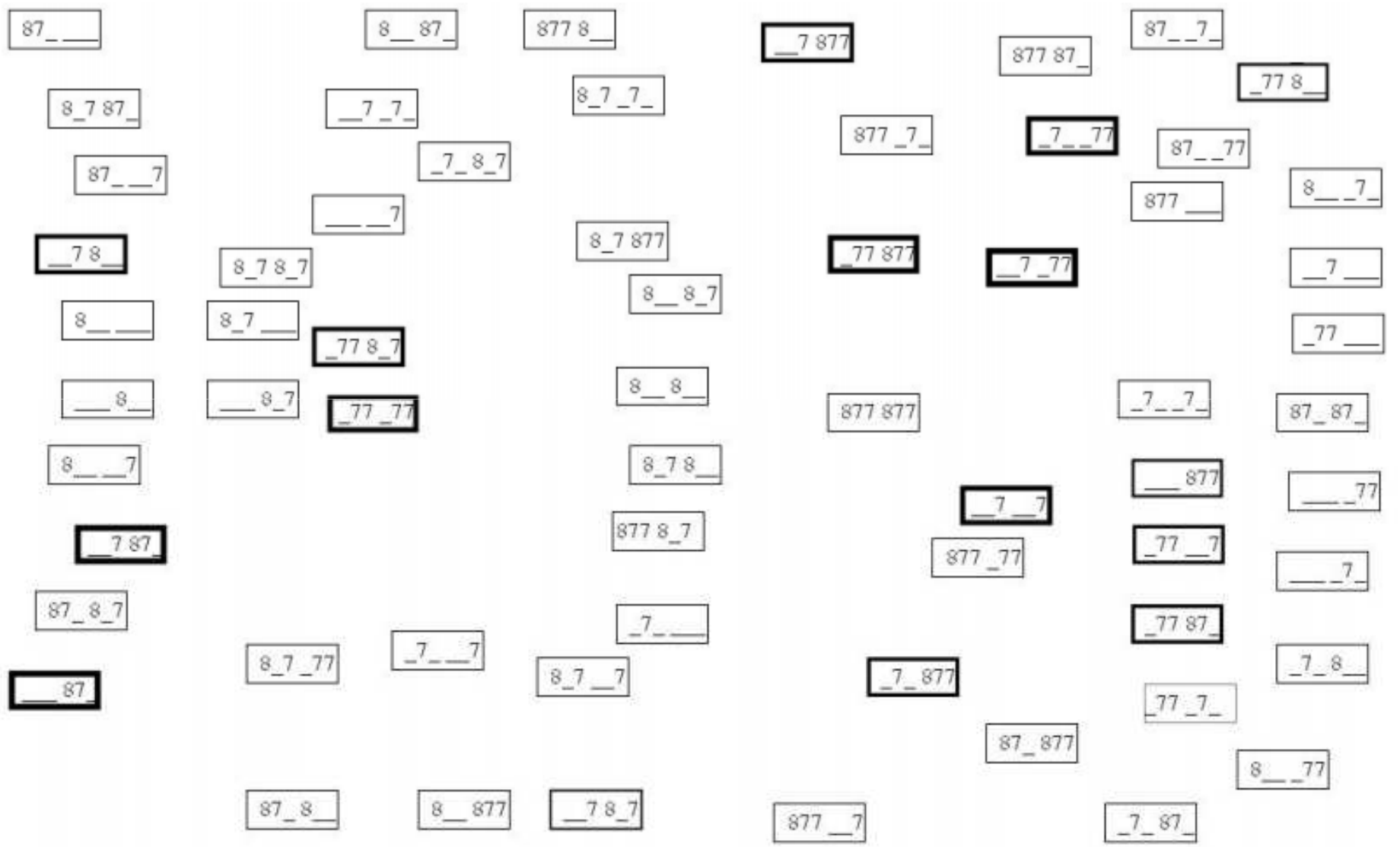


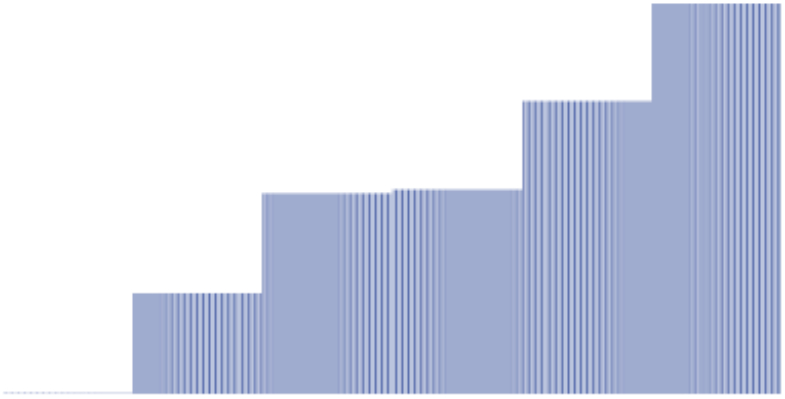
Figure 4: Propagation of (80000000, 00000000) after 8R

Low Entropy!

Figure 5: The Entropy estimation and plot after 1-7 rounds of GOST starting from the input set 8000000000000000

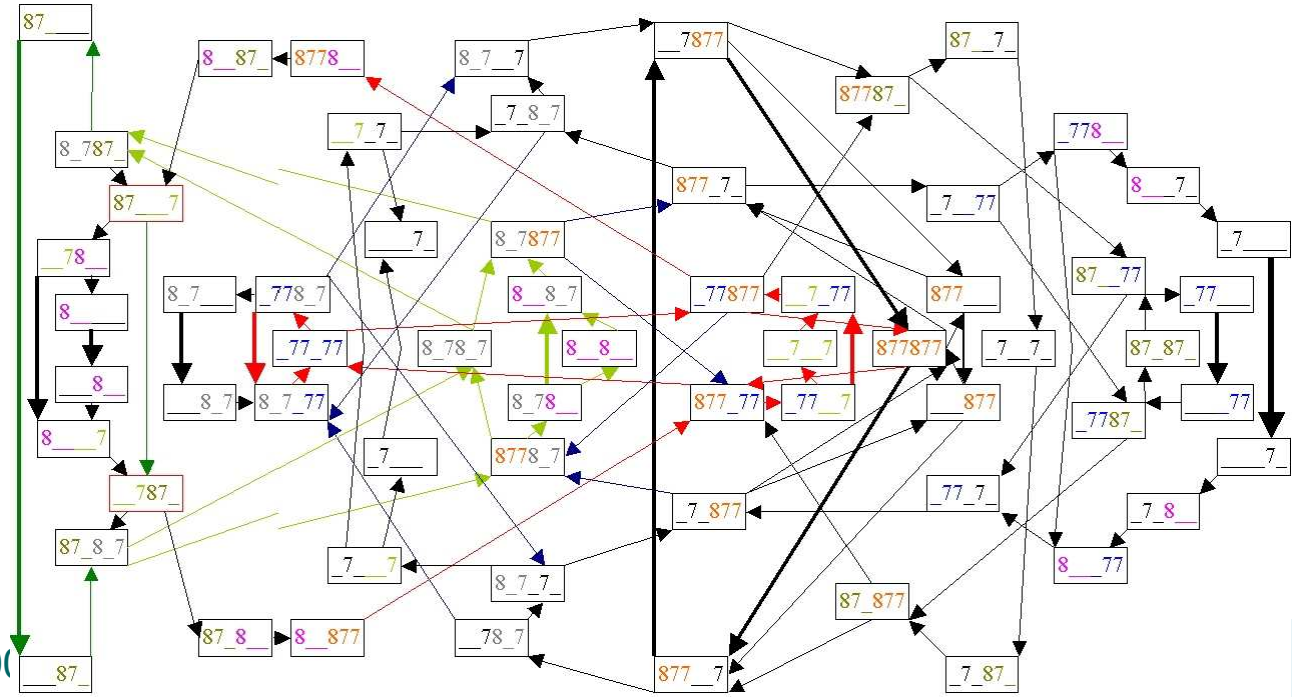
Round	Entropy
0	0.0
1	0.0
2	2.81
3	5.61
4	5.72
5	8.19
6	10.92
7	12.31

14 for RP



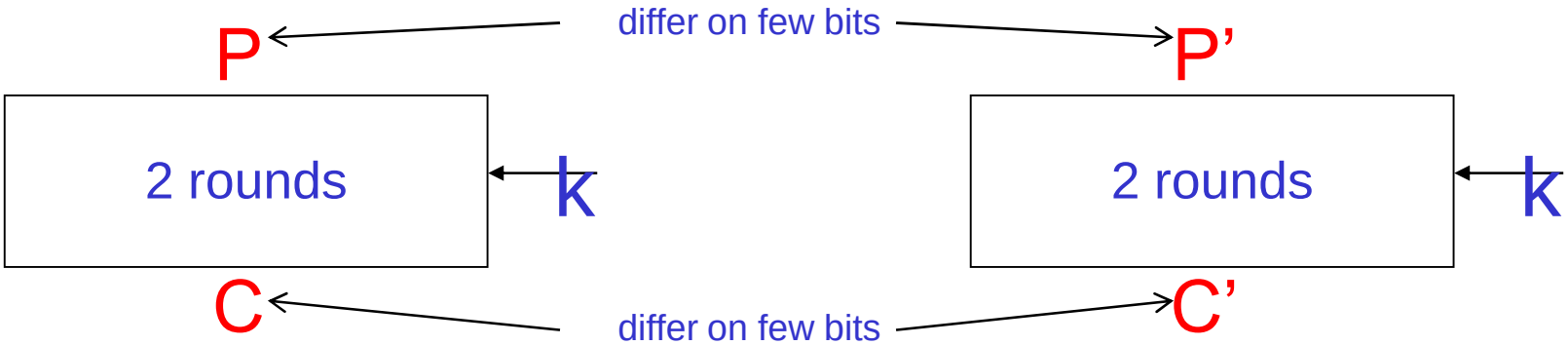
Remark:

- the structure of this graph does NOT depend on the S-boxes
- only costs (probabilities) depend on the S-boxes and not always a lot



14.4.1.
Truncated Differentials
As Collisions and Statistical Tests

"Truncated Differentials" == Double Collisions



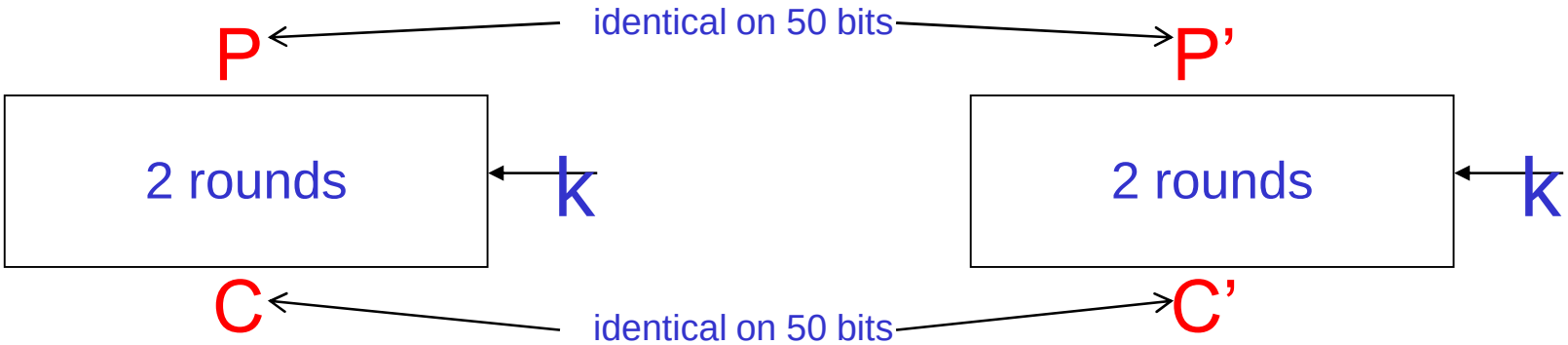
Proposed as "collision tests" in:

Cryptographic Randomness Testing of Block Ciphers and Hash Functions

eprint.iacr.org/2010/564

Ali Doğanaksoy, Barış Ege, Onur Koçak and Fatih Sulak

For GOST

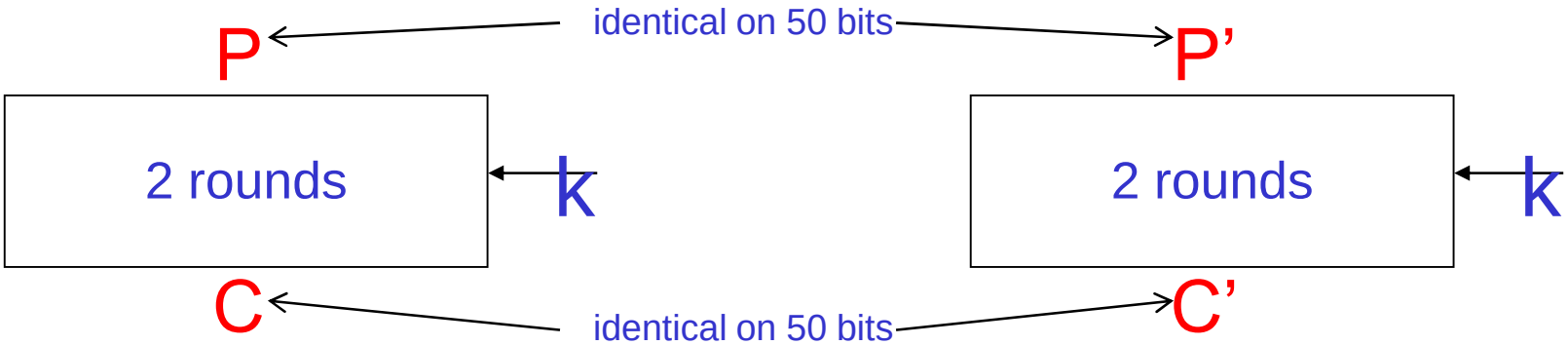


0x80700700,0x80700700

Cf.

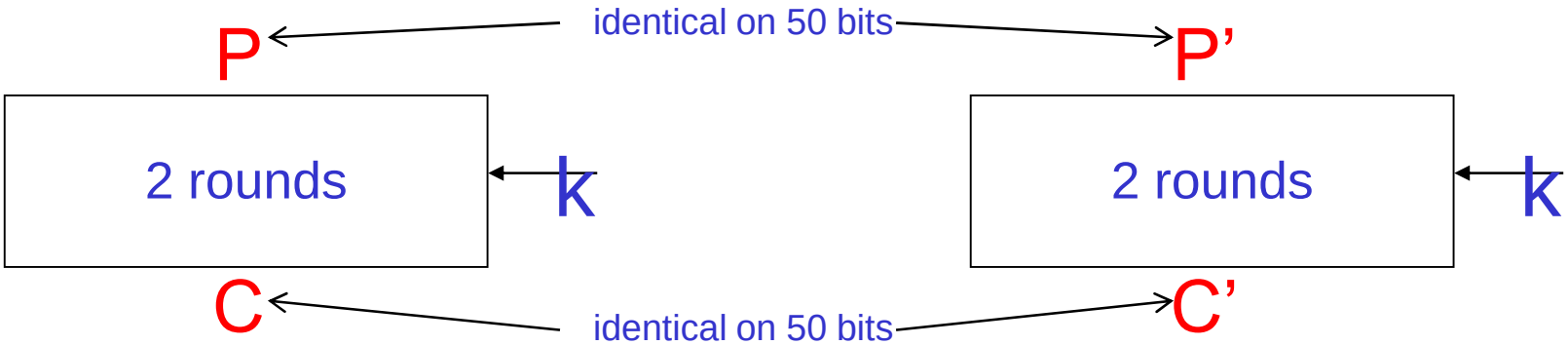
Nicolas T. Courtois, Michal Misztal: **Aggregated differentials and cryptanalysis of PP-1 and gost.** Periodica Mathematica Hungarica 65(2): 177-192 (2012)

What is Wrong?



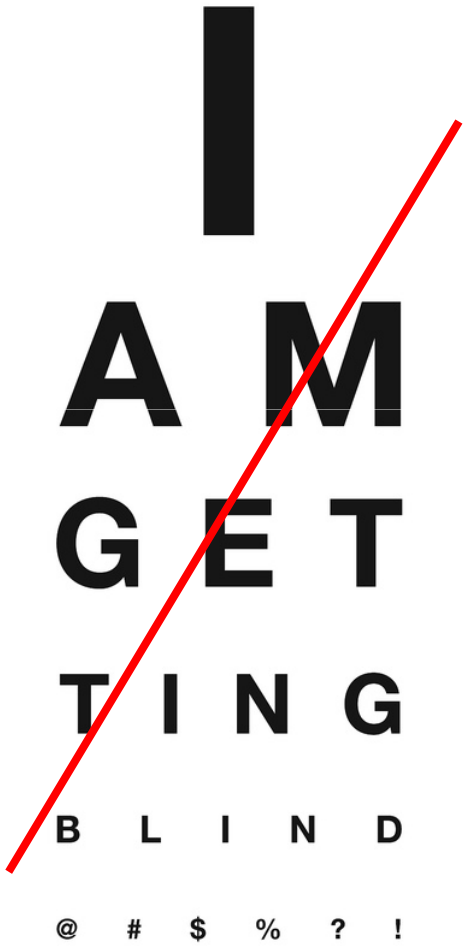
WRONG approach, or WRONG philosophy, or at least wrong vocabulary…

What is Wrong?

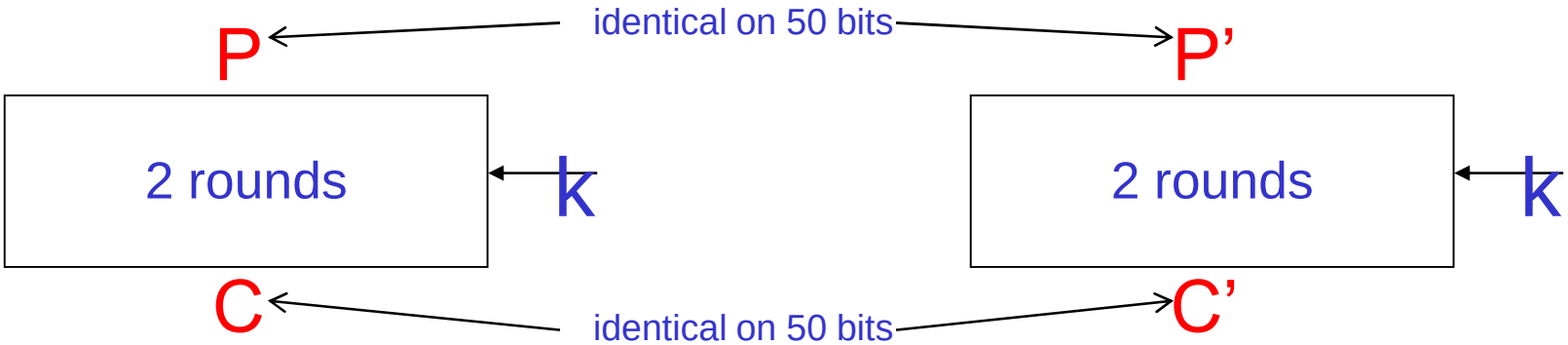


NOT a property to be TESTED at random (average case random testing).

Efficient Testing vs. Painful Discovery



Painful Discovery!



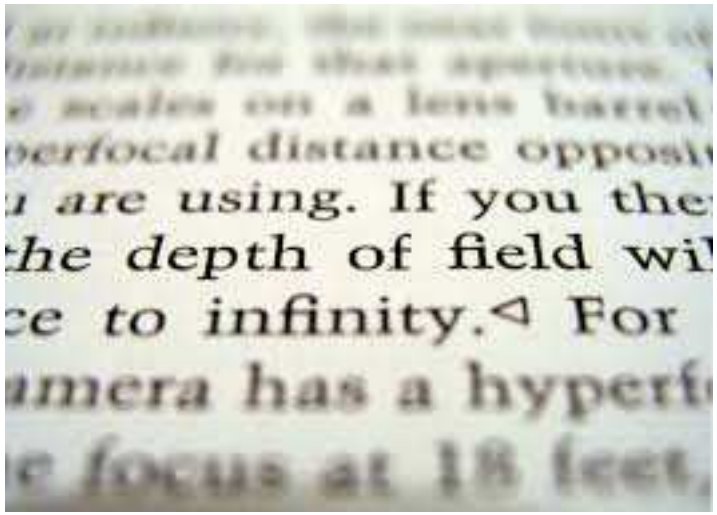
NOT a property to be TESTED for.

This property must be studied as the BEST case.

Can be difficult to find even if it exists.

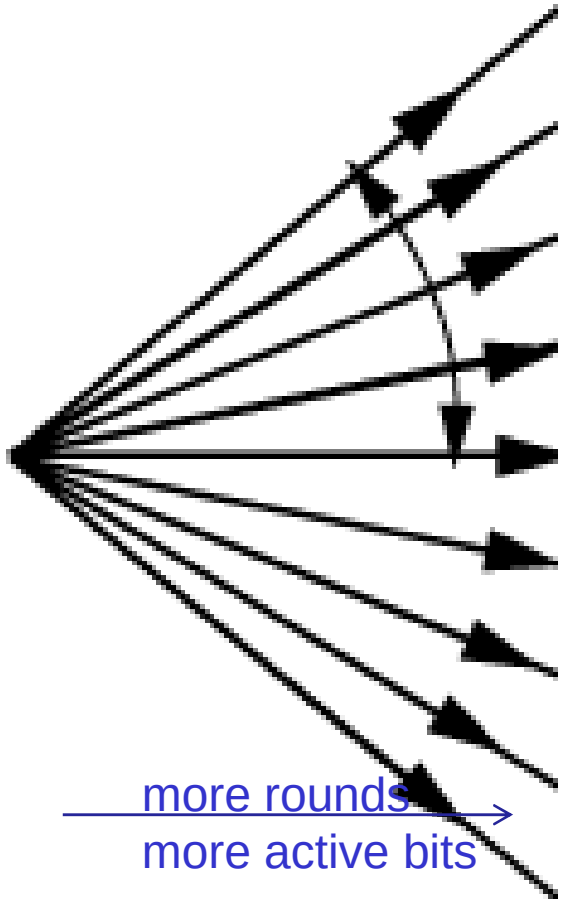
Moreover, size matters! As we will see later…

14.4.2.
Existence of Interesting Attacks



Philosophy (1)

One perturbation is always diffused in DC.

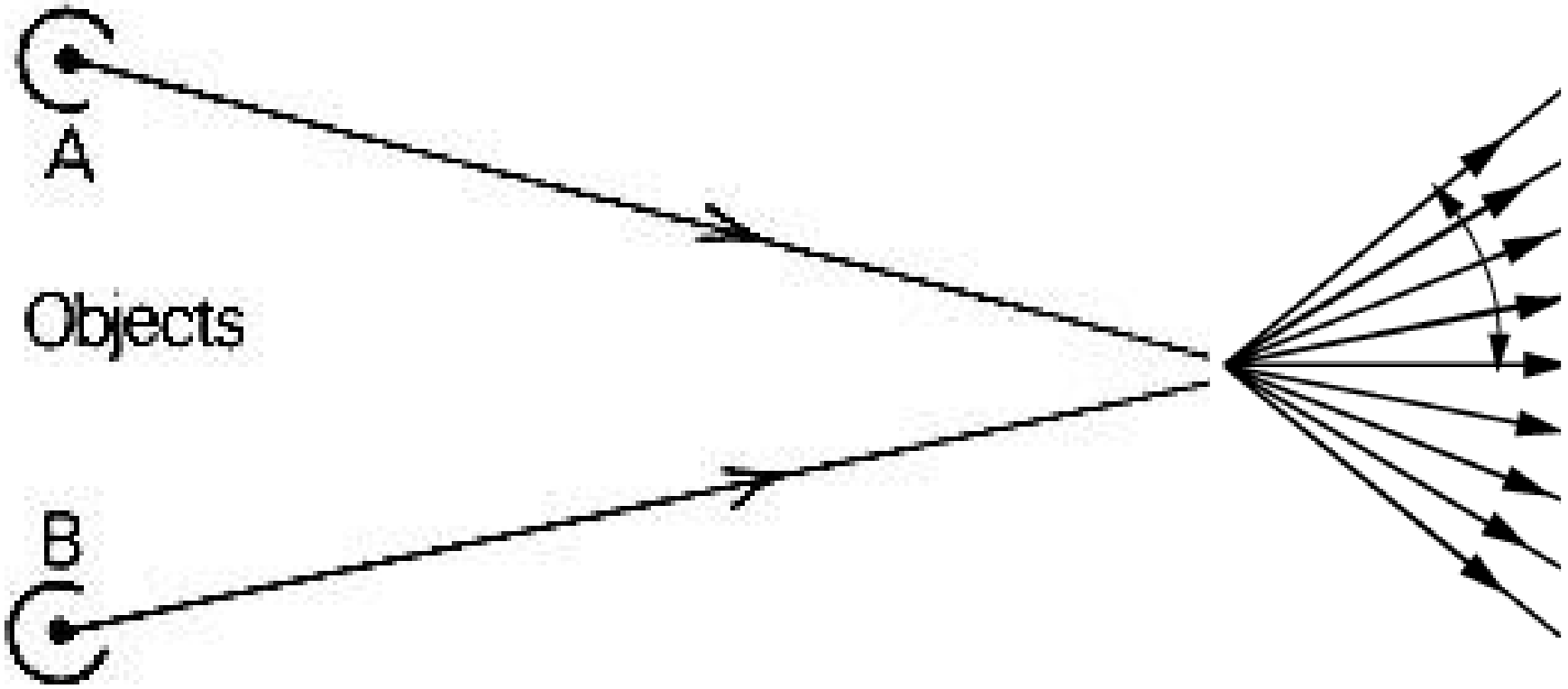


"diffusion cone"

ho hope it would be smaller…

Philosophy (2)

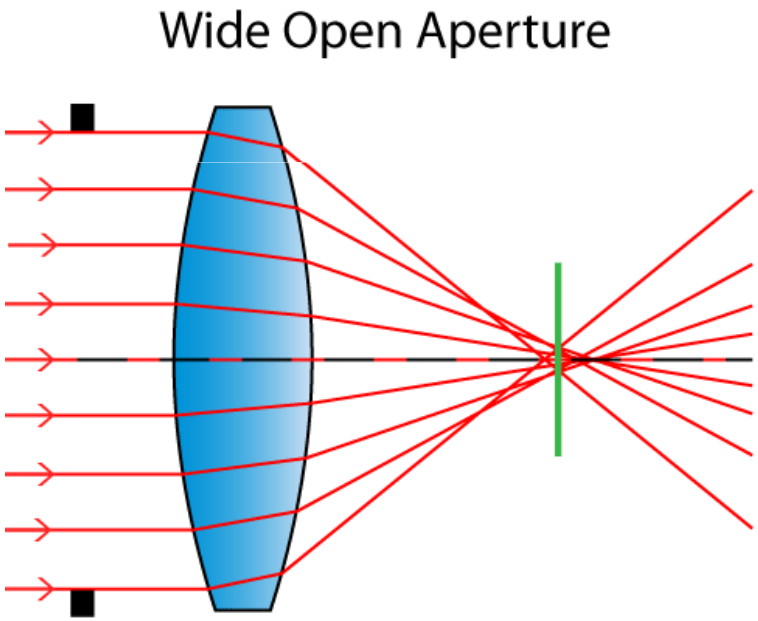
Can several perturbations converge somewhat? Like larger “channel capacity”.

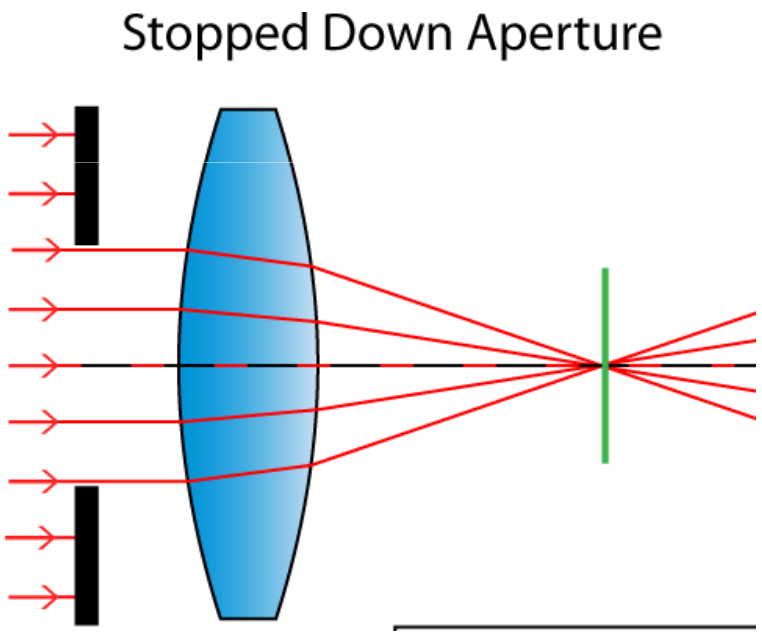


Philosophy (3)

Not if we have TOO many sources!

Must restrict the input diversity.





14.4.3.
From Existence to Discovery

Black Box Methods

Random guessing + several feedback/learning loops (evolutionary algorithm):

- flip few bits
- extend size
- decrease size
- use repeated “patters” seen
- etc…

Some Results – 19 bits,

"very good for 8R and good for 12R"

	S-box Set Name	Truncated differential set S	P([S]→[S]) 8R	12R
0	GostR3411_94_TestParamSet	78001078 07070780	$2^{-24.9}$	2^{-43}
1	GostR3411_94_CryptoProParamSet	08070780 78788030	$2^{-24.4}$	2^{-40}
2	Gost28147_TestParamSet	84000707 E0787200	$2^{-23.6}$	2^{-39}
3	Gost28147_CryptoProParamSetA	78780820 00070707	$2^{-25.2}$	2^{-42}
4	Gost28147_CryptoProParamSetB	80707820 07000787	$2^{-25.9}$	2^{-42}
5	Gost28147_CryptoProParamSetC	78780080 80070707	$2^{-25.5}$	2^{-43}
6	Gost28147_CryptoProParamSetD	84000787 70707800	$2^{-25.4}$	2^{-43}
7	GostR3411_94_SberbankHash	90000607 D4787800	$2^{-24.9}$	2^{-43}
8	GOST ISO 18033-3 proposal	80000707 F0787800	$2^{-23.8}$	2^{-43}
9	GOST-P proposal	F0707000 07000707	$2^{-27.0}$	2^{-44}

14.5.
Discovery of OPTIMAL Size [and Shape]

Nicolas T. Courtois, Michal Misztal: **Aggregated differentials and cryptanalysis of PP-1 and gost.** Periodica Mathematica Hungarica 65(2): 177-192 (2012)

Different Sizes

"very good for 8R"

a		GOST S-box Set Name	Truncated differential set S	P([S]→[S]) **8R**
24	0	GostR3411_94_TestParamSet	F0780780 F0070781	$2^{-28.3}$
21	0	GostR3411_94_TestParamSet	78780000 F0070783	$2^{-26.6}$
19	0	GostR3411_94_TestParamSet	78001078 07070780	$2^{-24.9}$
17	0	GostR3411_94_TestParamSet	D0707000 80000787	$2^{-23.7}$
15	0	GostR3411_94_TestParamSet	80707800 80000707	$2^{-22.9}$
14	0	GostR3411_94_TestParamSet	80707800 80000307	$\mathbf{2^{-22.6}}$
12	0	GostR3411_94_TestParamSet	80707800 80000007	$2^{-22.8}$
9	0	GostR3411_94_TestParamSet	80700780 80000000	$2^{-25.2}$
24	3	Gost28147_CryptoProParamSetA	F0770700 F0700708	2^{-31}
21	3	Gost28147_CryptoProParamSetA	78780060 80070787	$2^{-25.4}$
19	3	Gost28147_CryptoProParamSetA	78780820 00070707	$2^{-25.2}$
17	3	Gost28147_CryptoProParamSetA	03070780 78008070	$2^{-24.2}$
14	3	Gost28147_CryptoProParamSetA	70780000 80030780	$\mathbf{2^{-23.8}}$
12	3	Gost28147_CryptoProParamSetA	70780000 80080700	$2^{-26.7}$

Comparison With DES

"very good for 4R"

a	Reference Cipher	Truncated differential set S	P([S]→[S]) **4R**
17	U.S. Data Encryption Standard	D8081040 85308C06	$2^{-21.0}$
14	U.S. Data Encryption Standard	10001040 85118C26	$2^{-18.8}$
12	U.S. Data Encryption Standard	80521890 04200802	$2^{-18.8}$
11	U.S. Data Encryption Standard	A05000B0 04200802	$\mathbf{2^{-16.4}}$
10	U.S. Data Encryption Standard	00802080 0C080A0A	$\mathbf{2^{-16.8}}$
9	U.S. Data Encryption Standard	08020000 80F88000	$\mathbf{2^{-16.7}}$
8	U.S. Data Encryption Standard	08020000 80B88000	$\mathbf{2^{-16.6}}$
7	U.S. Data Encryption Standard	08020000 80B80000	$2^{-16.8}$
6	U.S. Data Encryption Standard	4000008B 00040000	$2^{-17.3}$
5	U.S. Data Encryption Standard	005000B0 14200800	$2^{-18.1}$

Another Block Cipher

D	Reference Cipher	Truncated differential set S	$P([S]\rightarrow[S])$ **4R**
11	TEA = Tiny Encryption Algorithm	008008A0 81009111	2^{-13}
10	TEA = Tiny Encryption Algorithm	00010012 90001131	$\mathbf{2^{-11}}$
9	TEA = Tiny Encryption Algorithm	80600034 00800101	$\mathbf{2^{-11}}$
8	TEA = Tiny Encryption Algorithm	4A000112 01000001	$\mathbf{2^{-11}}$
6	TEA = Tiny Encryption Algorithm	00200020 001000A1	2^{-13}

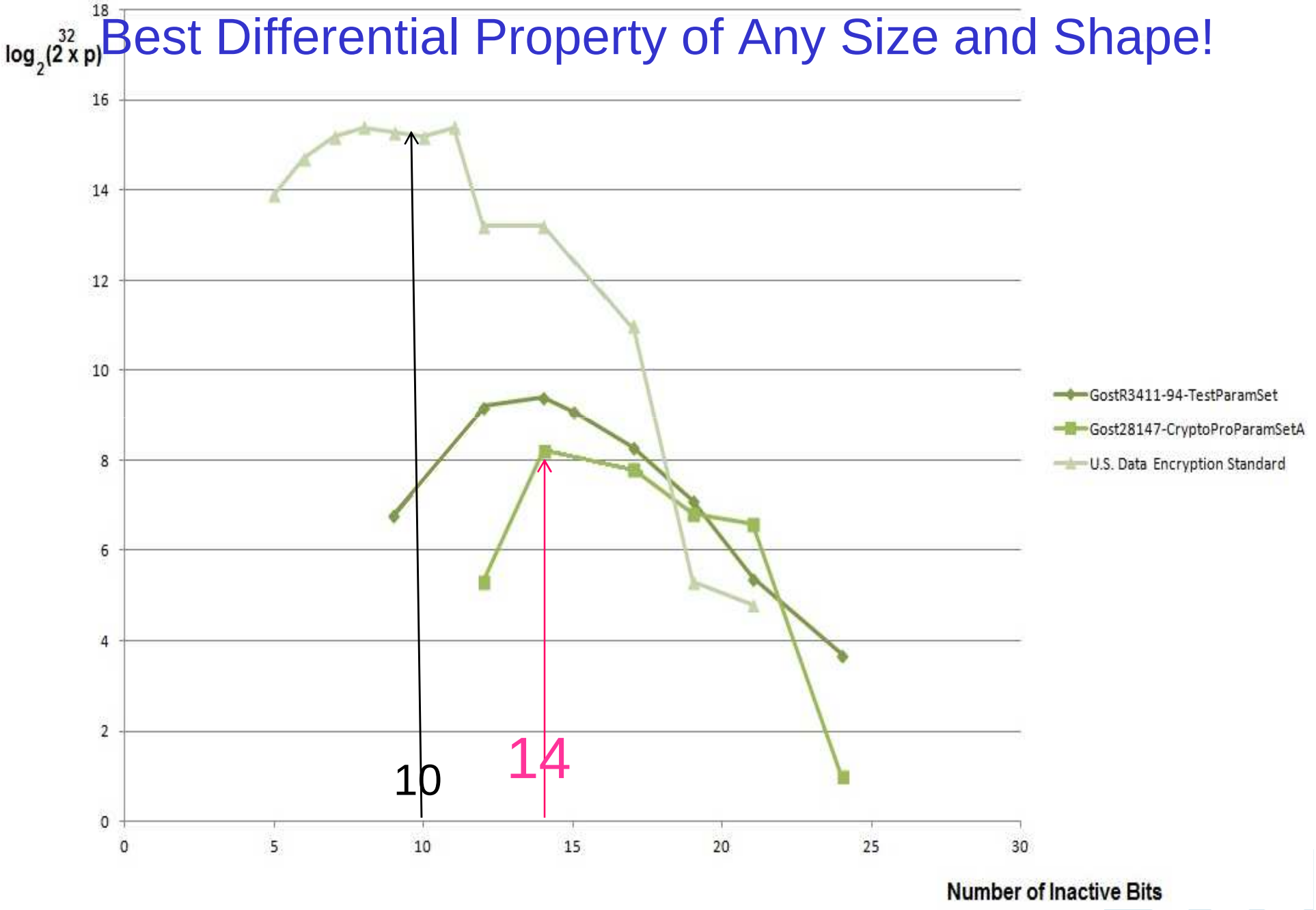
Some Results – 14 bits,

"very good for 8R"

Table 1: Some recent results with sets of 14 bits and 8 rounds cf. [10]

Set Name	Set	P(8R)
default set [21]	78000078 07070780	$2^{-24.0}$
ISO 18033-3 proposal	80000707 20707000	$2^{-22.7}$

Best Differential Property of Any Size and Shape!



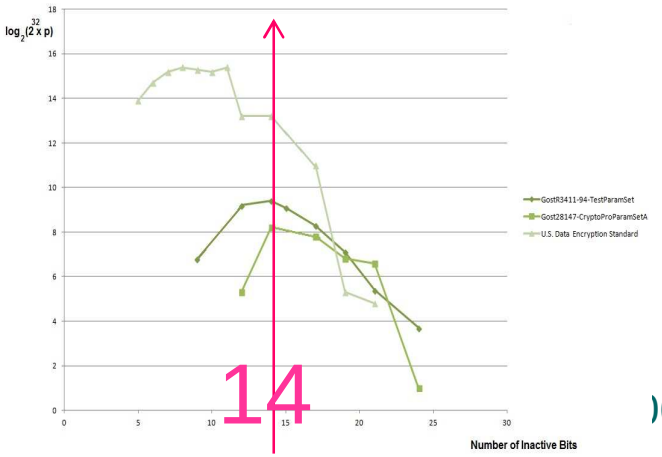
Best Differential for GOST = 14 Bits

⇒14 bit properties discovered earlier:

Nicolas T. Courtois, Michal Misztal: **Aggregated differentials and cryptanalysis of PP-1 and gost.** Periodica Mathematica Hungarica 65(2): 177-192 (2012)

can be shown to be optimal !

⇒24 cannot be good



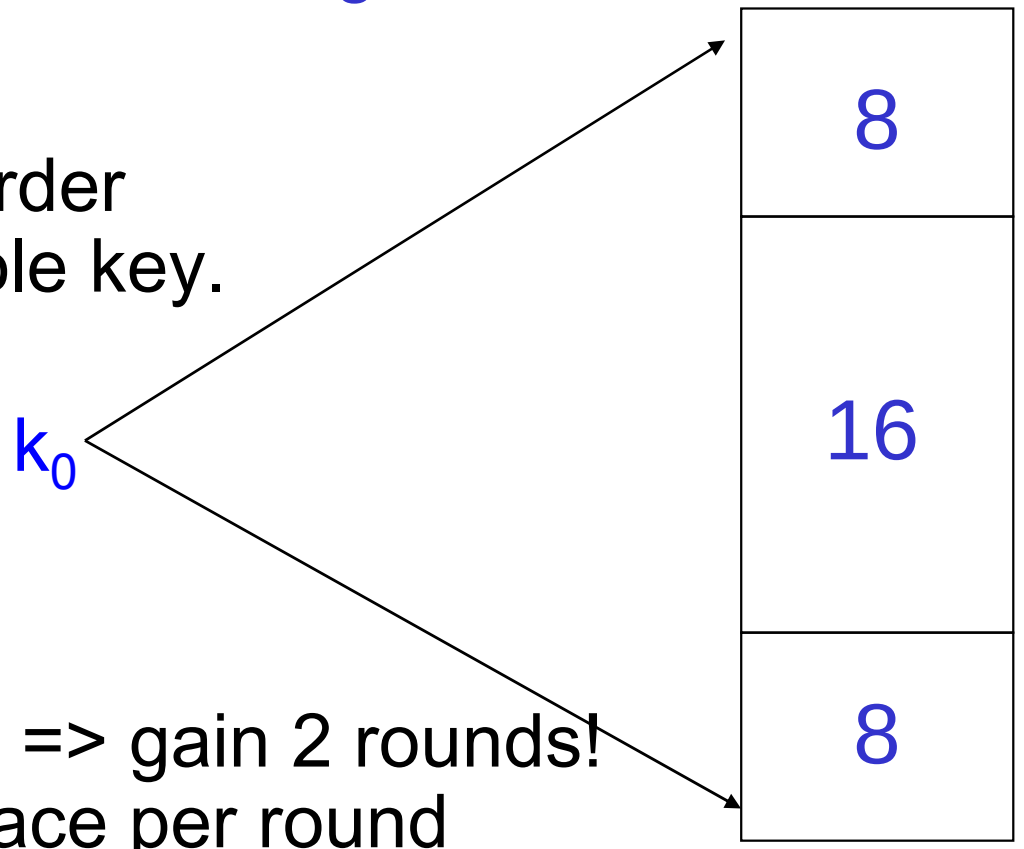
14.6.
DC -> Distinguishers
And Refined Attacks

Key Scheduling

Essential Weakness:

Same Keys Inversed Order

+ small size << whole key.



GOST: 32 bits guessed => gain 2 rounds!

- 0.06 of the key space per round

DES: 48 key bits guessed => 1 round

- 0.86 of the key space per round

New Attacks

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}