Cryptanalysis of GOST

Nicolas T. Courtois

University College London, UK

Outline

1. Cold War cryptography
2. GOST: Russian encryption standard
3. GOST submission to ISO in 2010
4. How GOST can eventually be broken…

   >60 distinct attacks… Best = 2^{101}

2011/626 updated

Main Themes:

1. Self-Similarity:
   extremely rich universe of distinct non-trivial attacks which generalize many known attacks but are non of these.
2. Algebraic Complexity Reduction:
   Magical “tricks” to black-box reduce an attack on a cipher with 32 rounds to an attack on 8 or 4 rounds.

Main Themes:

1. Self-Similarity:
   extremely rich universe of distinct non-trivial attacks which generalize many known attacks but are non of these.
2. Algebraic Complexity Reduction:
   Magical “tricks” to black-box reduce an attack on a cipher with 32 rounds to an attack on 8 or 4 rounds.

*Bonus: How to measure security:
discovery that single-key attacks are NOT the right notion to evaluate key length w.r.t. realistic attacks.

History: Cold War
Russia vs. USA

- My Favourite Groups

LinkedIn Account Type: Basic

Home Profile Contacts Groups Jobs Inbox 2 Companies News More

Your Groups (51) Reorder »

Create a

Code Breakers Members (311)

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

Data ENCRYPTION

IACR Cryptographers

Russian Subtitles On:

code breakers ==

ВЗЛОМЩИКИ КОДОВ

History: 1918

- Tzarist secret services

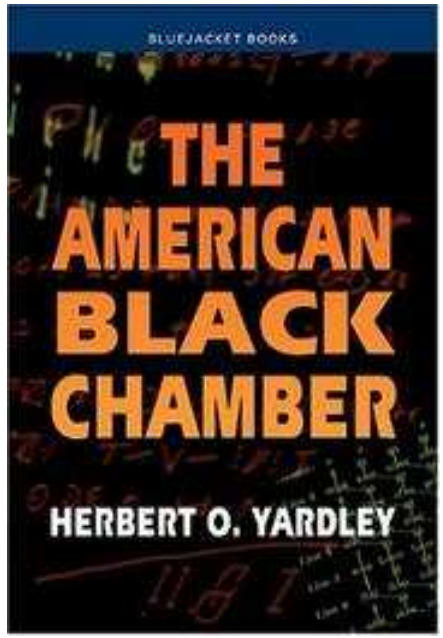
  => continued their work with the armies of white generals.

- In 1918 - 1920 almost all encrypted correspondence of the Soviet Army and Government was easily broken by
  - the white (counterrevolutionary) armed forces
  - the British
  - the Swedish
  - the Polish: broke key messages and won the War against Russia in 1920-1921

1930

1930: Russian code breaker Bokiy broke a U.S. code.

- US ciphers were really not good at that time…
  - In 1929 US government disbanded its Federal crypto services because… “Gentlemen don’t read each other’s mail”…



Fialka = Фиалка = Violet = M-125

Around 1965.

MUCH stronger than Enigma…

Used until 1987 in East Germany…

Fialka Versions

- Each country of the Warsaw pact had their own version
- Different keyboard, different fonts…
- Different SECRET set of 10 wheels.

Cold War Soviet Cryptanalysis

- Soviet Union was breaking codes and employed at least 100 cryptologists…

  [Source: Cryptologia, interviews by David Kahn with gen. Andreev=first head of FAPSI=Russian NSA]

Example: In 1967 GRU (Soviet Intelligence) was intercepting cryptograms from 115 countries, using 152 cryptosystems, and among these they broke 11 codes…

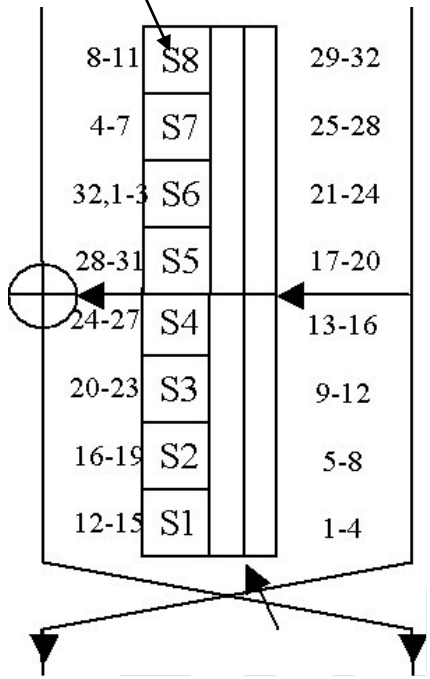
Was Fialka Broken?

- Israel have captured Fialka machines during the 6-day war in 1967 and … nothing more was disclosed.
- Austria would intercept and decrypt a fair proportion of Fialka traffic during the Cold War…
- In the 1970s the NSA would build a supercomputer to decrypt Fialka routinely

Secret Specs: ROTORS vs. S-boxes

FIALKA

GOST



Compare: Rotors of Enigma [1930s]

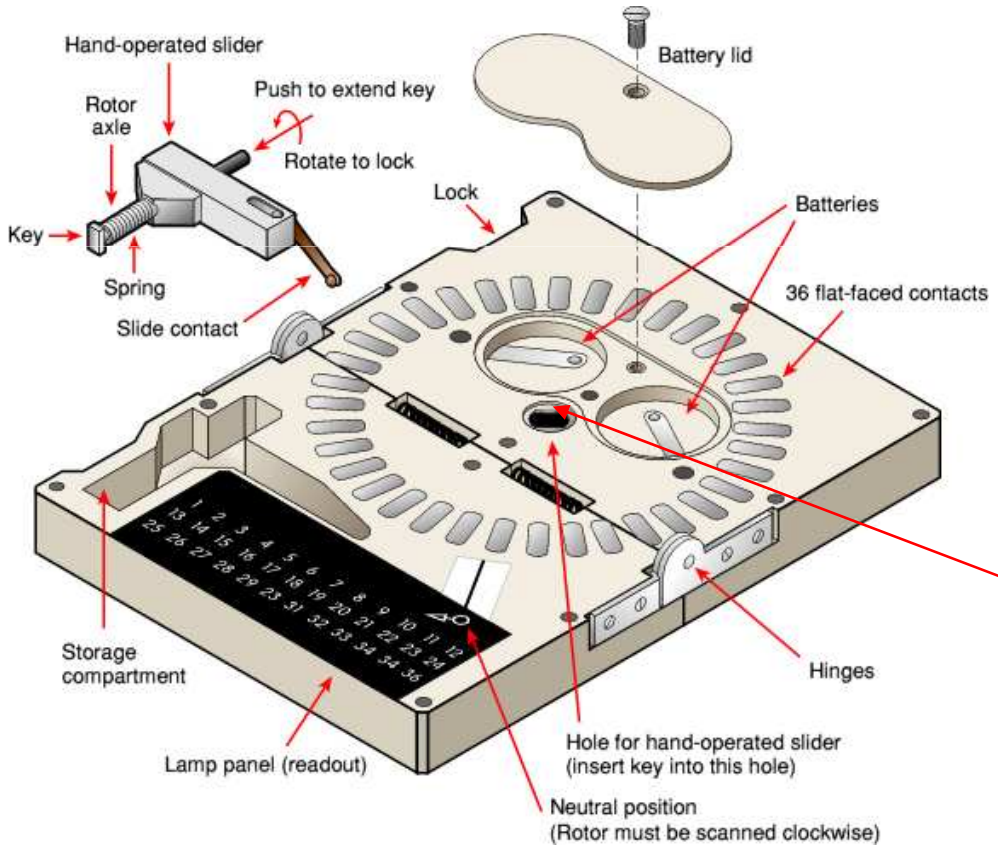
- The specs of Enigma were reverse-engineered by the Polish in early 1930s in tight collaboration with French intelligence… [and the British].
- Finding the rotors by Marian Rejewski was much harder than daily code breaking at Bletchley Park…

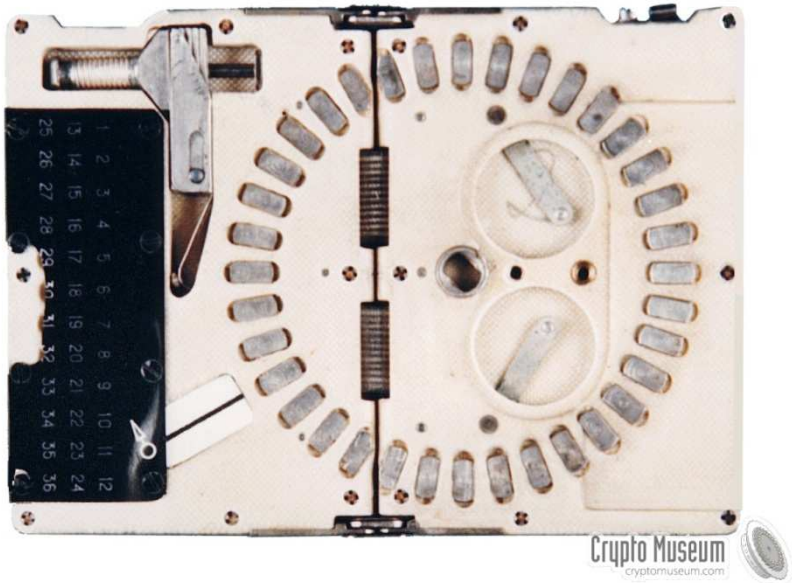
US Ciphers

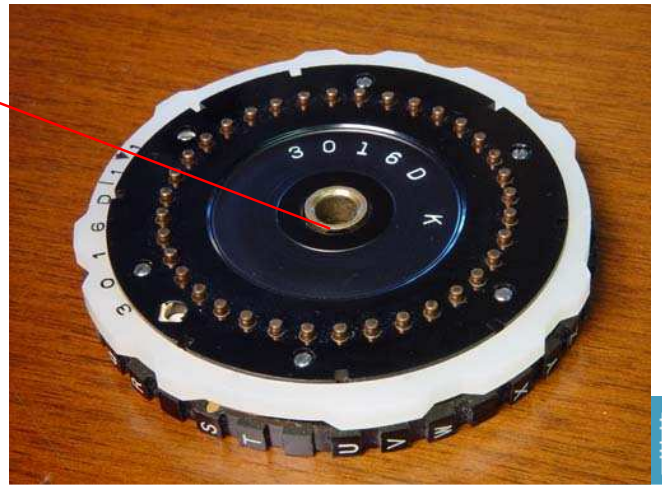
- US/NATO:
  Russia broke the NATO KL-7 cipher machine
  - the NSA did not see it was weak…
  - The spec became known because of a spy ring
    - by John A .Walker Jr + family.
    - was paid more than 1M USD (source: NSA)
    - to this day the spec has NOT been made public
  - greatest exploit in KGB history,
  - allowed the Soviet Union to “read millions” of American messages [1989, Washington Post]

Walker Amazing Machine

Walker obtained from the KGB a pocket machine to read the connections of rotors of KL-7







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 

Two Worlds:

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

    => Low data complexity

Algebraic Attacks on Block Ciphers

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

Ready Software for Windows

Ready programs:

www.cryptosystem.net/aes/tools.html

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/

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

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

And GOST?

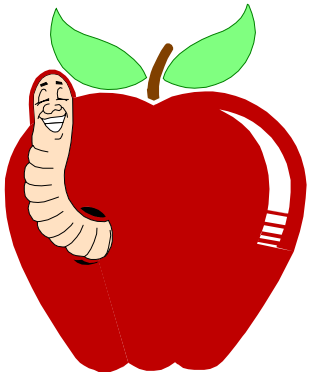
Essentially the same software methods…

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



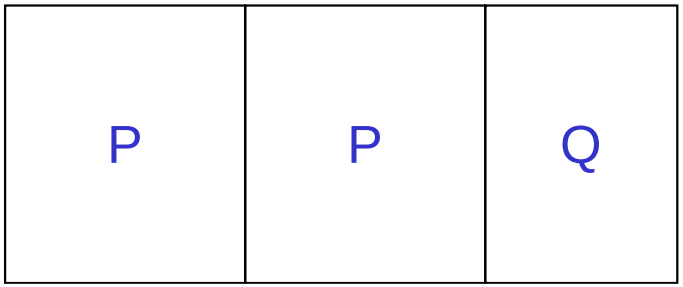
or What's Wrong With Some Ciphers

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]

“Courtois Dark Side” Attack on MiFare Classic

Cf. eprint.iacr.org/2009/137. Basic Facts:

It is a multiple differential attack.

Also a “self-similarity” attack.

>2 billions smart cards sold…

Still massively used by 100s of millions of people…

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$.

4.4. Sliding Properties of KeeLoq

[and one simple attack from FSE 2008]

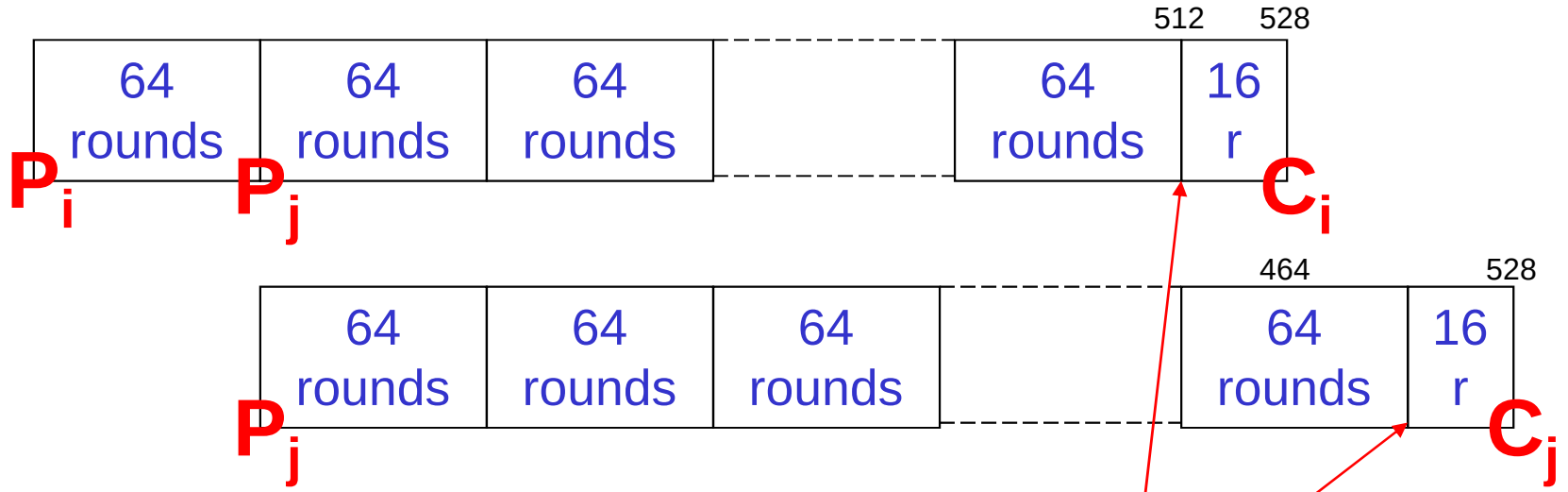
Sliding Attacks

Classical Sliding Attack
[Grossman-Tuckerman 1977]:

Gives an unlimited number of other sliding pairs !!!

Classical Sliding –Not Easy

Classical sliding fails…

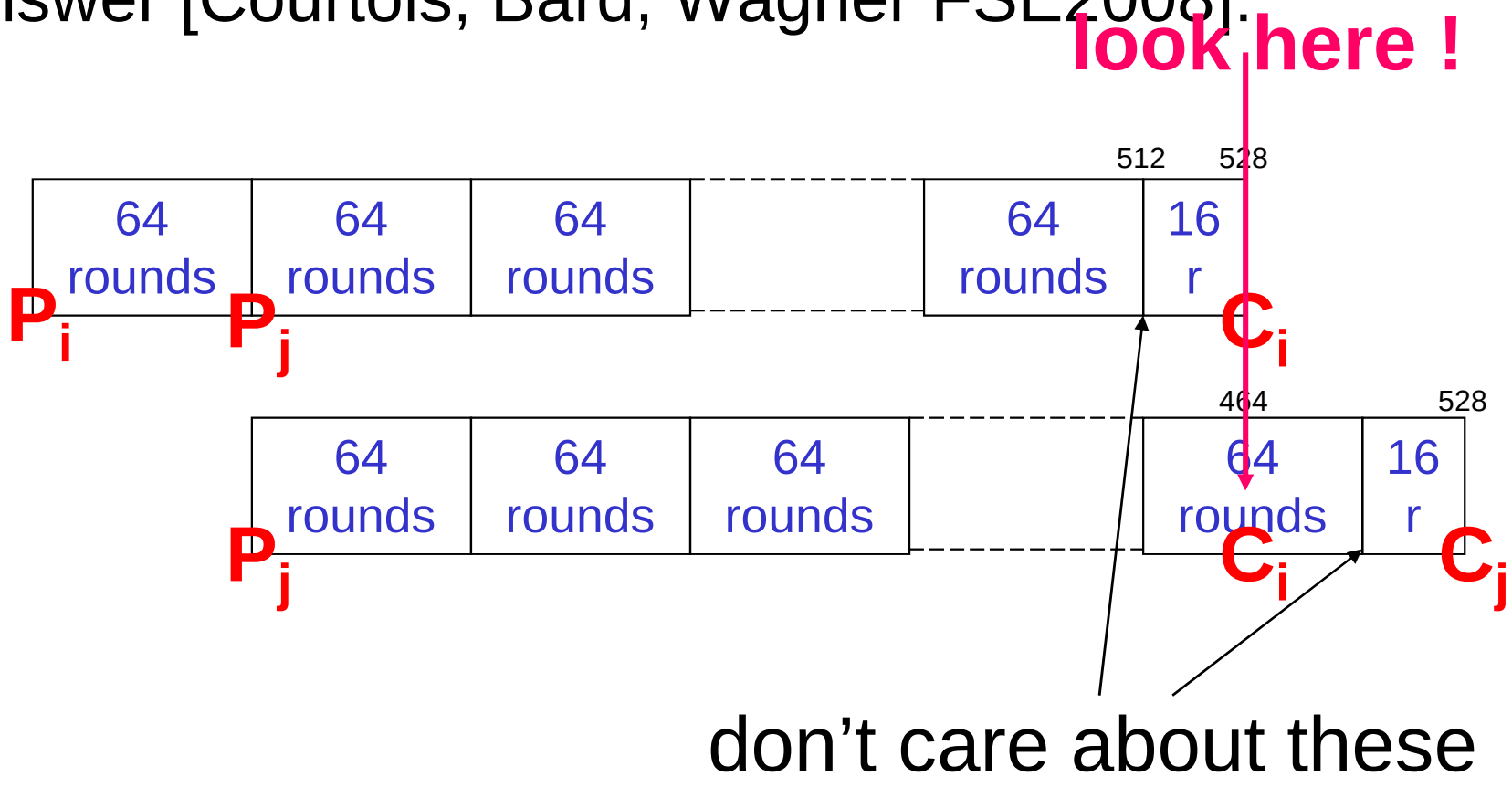


HARD - Problem:

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

- Solve it.
  - Takes 2 seconds on a PC withn a SAT solver.

Attack Summary:

Data = 2^{16} KP.

Time = 2^{53}.

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.
  - Later: GOST also submitted in 2010…

Modular Addition

+ modulo 2^{32}

in several ciphers: GOST, SNOW 2.0.

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

Modular Addition I/O Degree = 2

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

(the c_i can be all eliminated)

$$(*)\begin{cases} z_0 = x_0 + y_0 \\ z_1 = x_1 + y_1 + c_1 \\ z_2 = x_2 + y_2 + c_2 \\ \vdots \\ z_i = x_i + y_i + c_i \\ \vdots \\ z_{n-1} = x_{n-1} + y_{n-1} + c_{n-1}, \end{cases} \qquad (*')\begin{cases} c_1 = x_0 y_0 \\ c_2 = x_1 y_1 + (x_1 + y_1)c_1 \\ \vdots \\ c_i = x_{i-1} y_{i-1} + (x_{i-1} + y_{i-1})c_{i-1} \\ \vdots \\ c_{n-1} = x_{n-2} y_{n-2} + (x_{n-2} + y_{n-2})c_{n-2} \end{cases}$$

4.7. High-Level Attacks on Snow 2.0.

[Courtois-Debraize ICICS 2008]

idea

We want to fix some WELL CHOSEN bits, determine other.

How? Structure of Snow dictates that.

Amplification=4 or How to Linearize Snow?

Fix to 0.

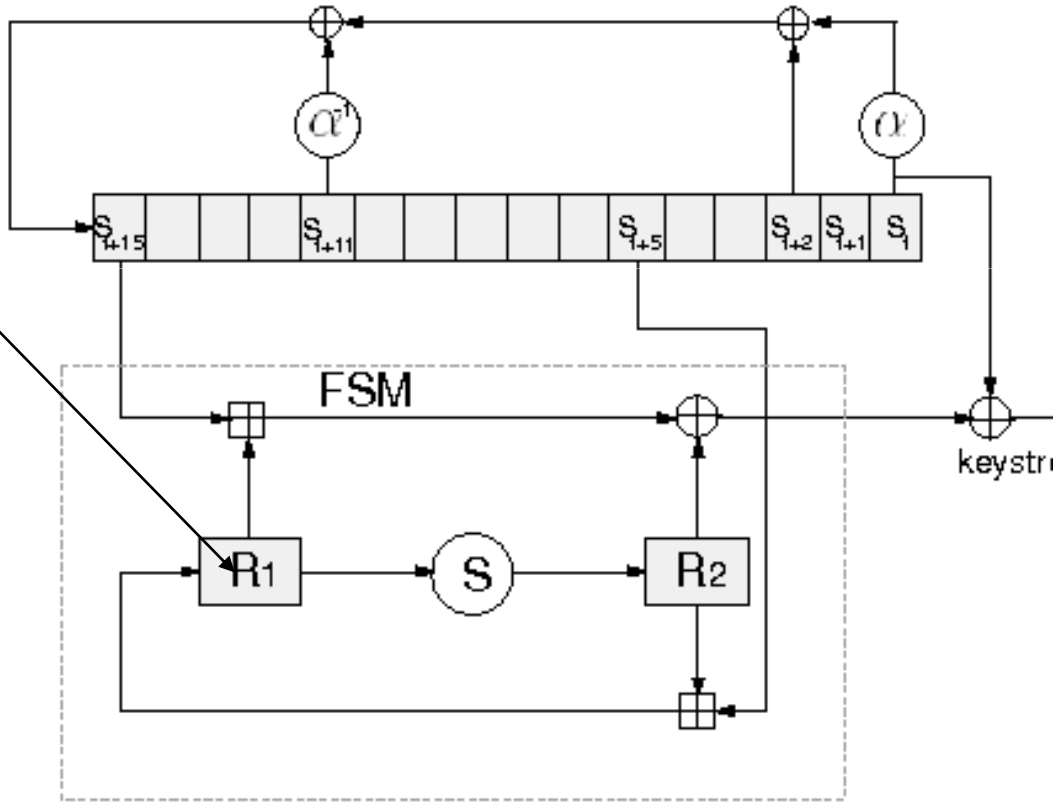
For 9 consecutive steps.

Linearizes both +!

And the S-box layer

n -> 4n equations.

Seems optimal.



5. GOST Cipher

GOST 28148-89

- The Official Encryption Standard of Russian Federation.
- Developed in the 1970s (?)
  - Former "Top Secret" algorithm.
  - Declassified in 1994.

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

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 assume known S-boxes.
  - there are papers 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…

[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"

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

- Standard GOST:
  - Only 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, Snow, PRESENT.

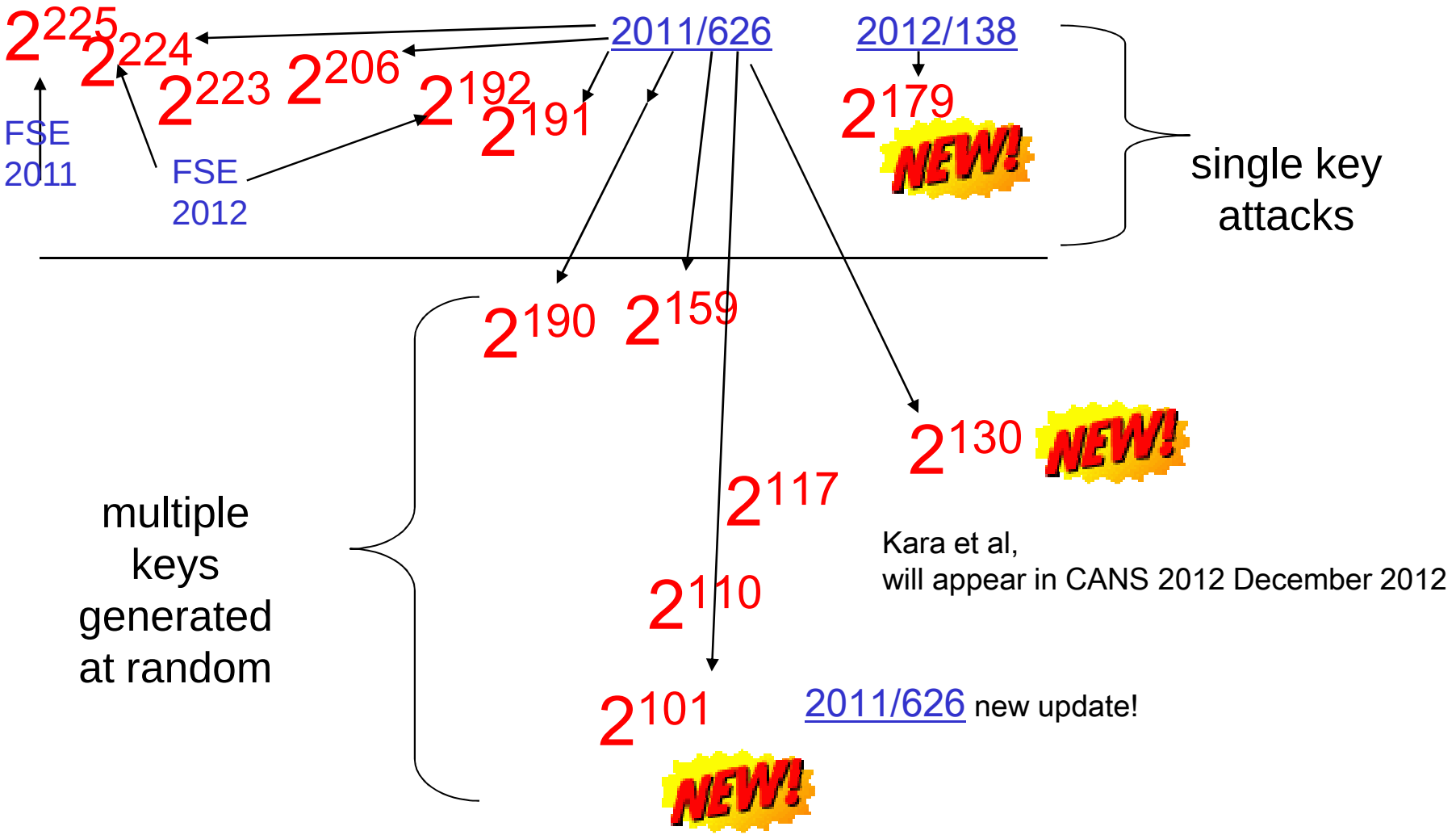
GOST in ISO

- 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].

Future of GOST in ISO

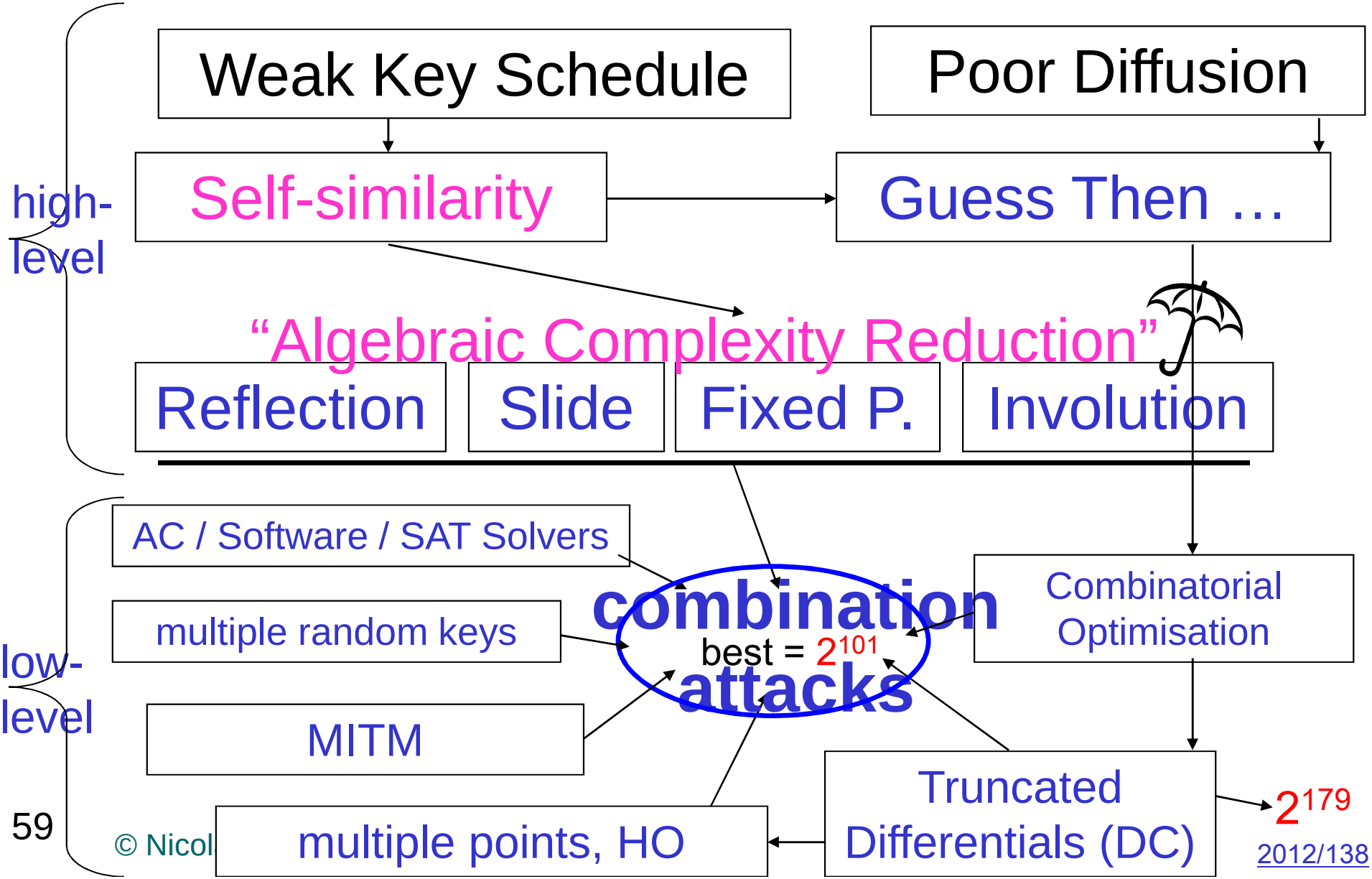
- Our report [eprint/2011/211] was officially submitted to ISO.
- It says: […] to standardize GOST now would be really dangerous and irresponsible […]
- But Why?
  - Half-broken in very serious sense
  - Really broken in academic sense

Development History



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

cf. 2011/626



6. Algebraic Complexity Reduction

Conditional AC

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

⇒ 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].

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	$\mathbf{k_0}k_1k_2k_3k_4k_5k_6k_7$	$\mathbf{k_0}k_1k_2k_3k_4k_5k_6k_7$	$\mathbf{k_0}k_1k_2k_3k_4k_5k_6k_7$	$k_7k_6k_5k_4k_3k_2k_1\mathbf{k_0}$

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 $\mathcal{E} \circ \mathcal{D} = \mathcal{D} \circ \mathcal{E} = Id$.

Last 16 Rounds of GOST

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

"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

$Q^{-1} \circ P \circ Q$

have the same cycle structure

Last 16 Rounds of GOST

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

"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 => attack on GOST with 2^{159} per key

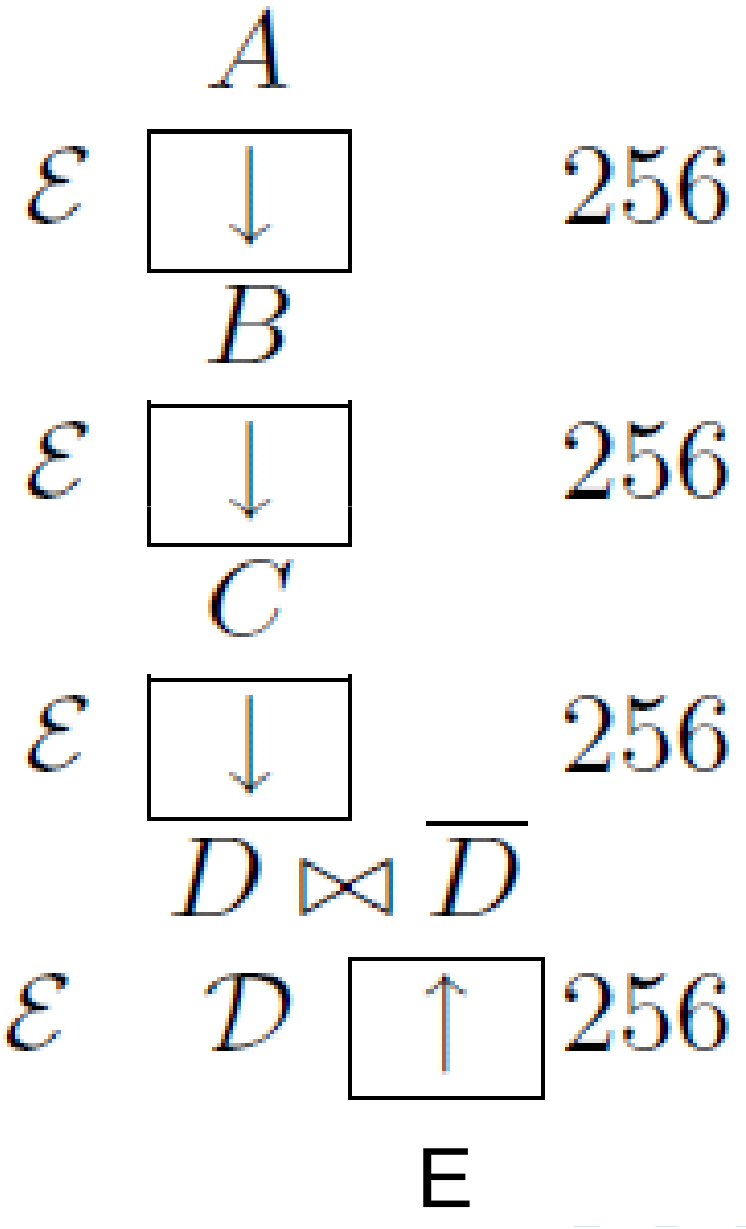
6.4. Complexity Reduction: First Example:

Relaxing the Requirements of A Sliding Attack

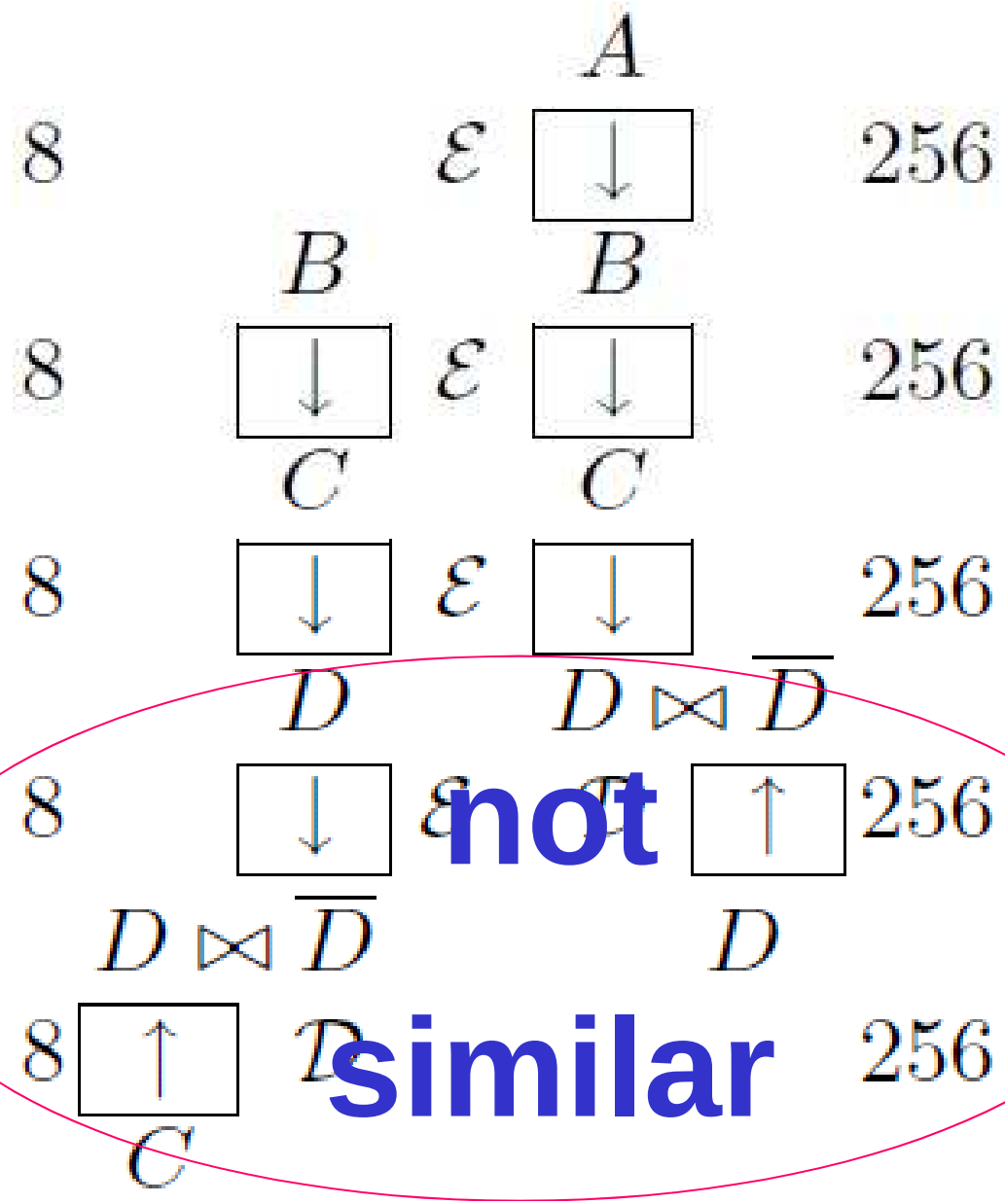
Black Box Reduction: Pseudo-Sliding Attack [Cryptologia Jan 2012]

One Encryption

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



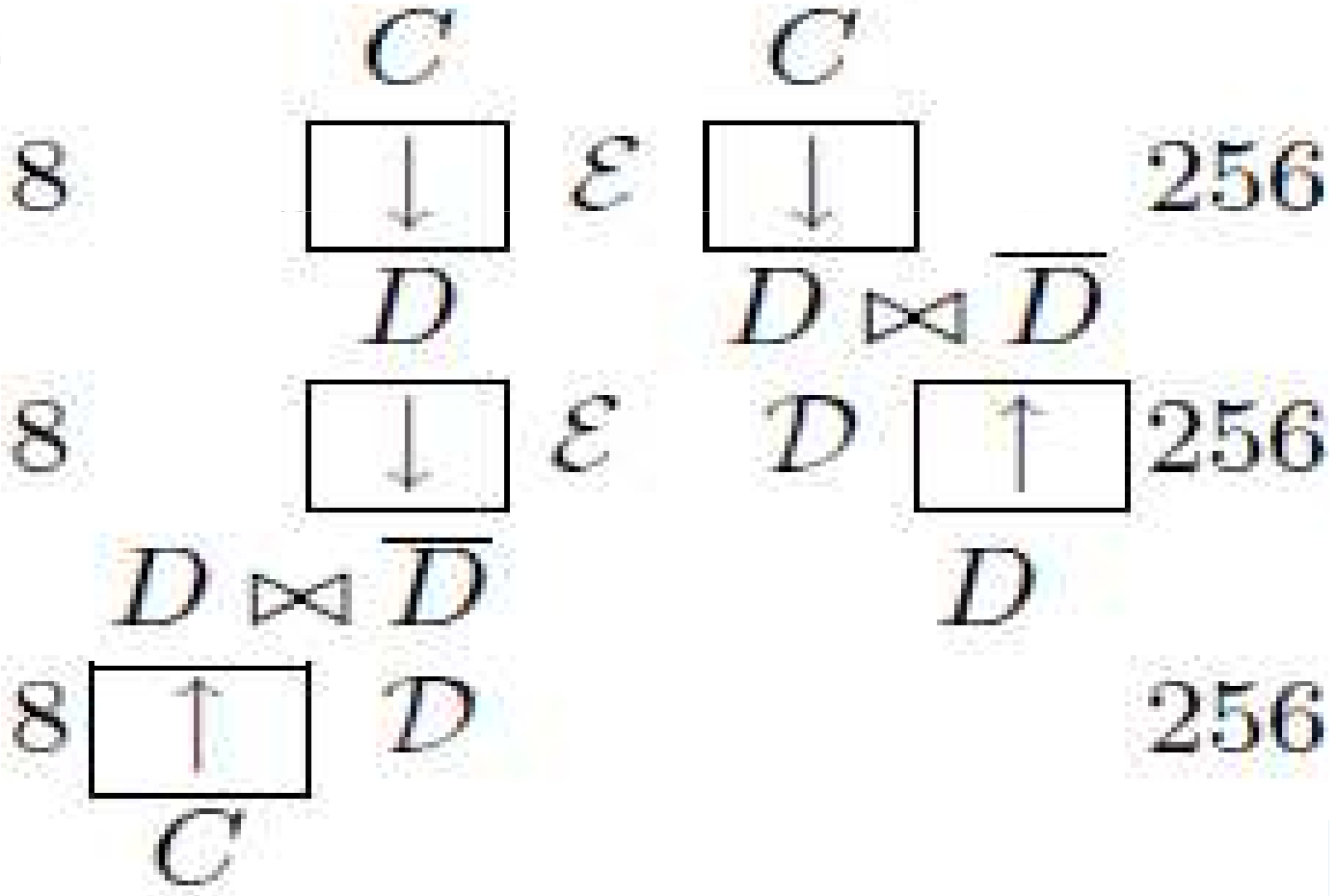
Two Encryptions with A Slide

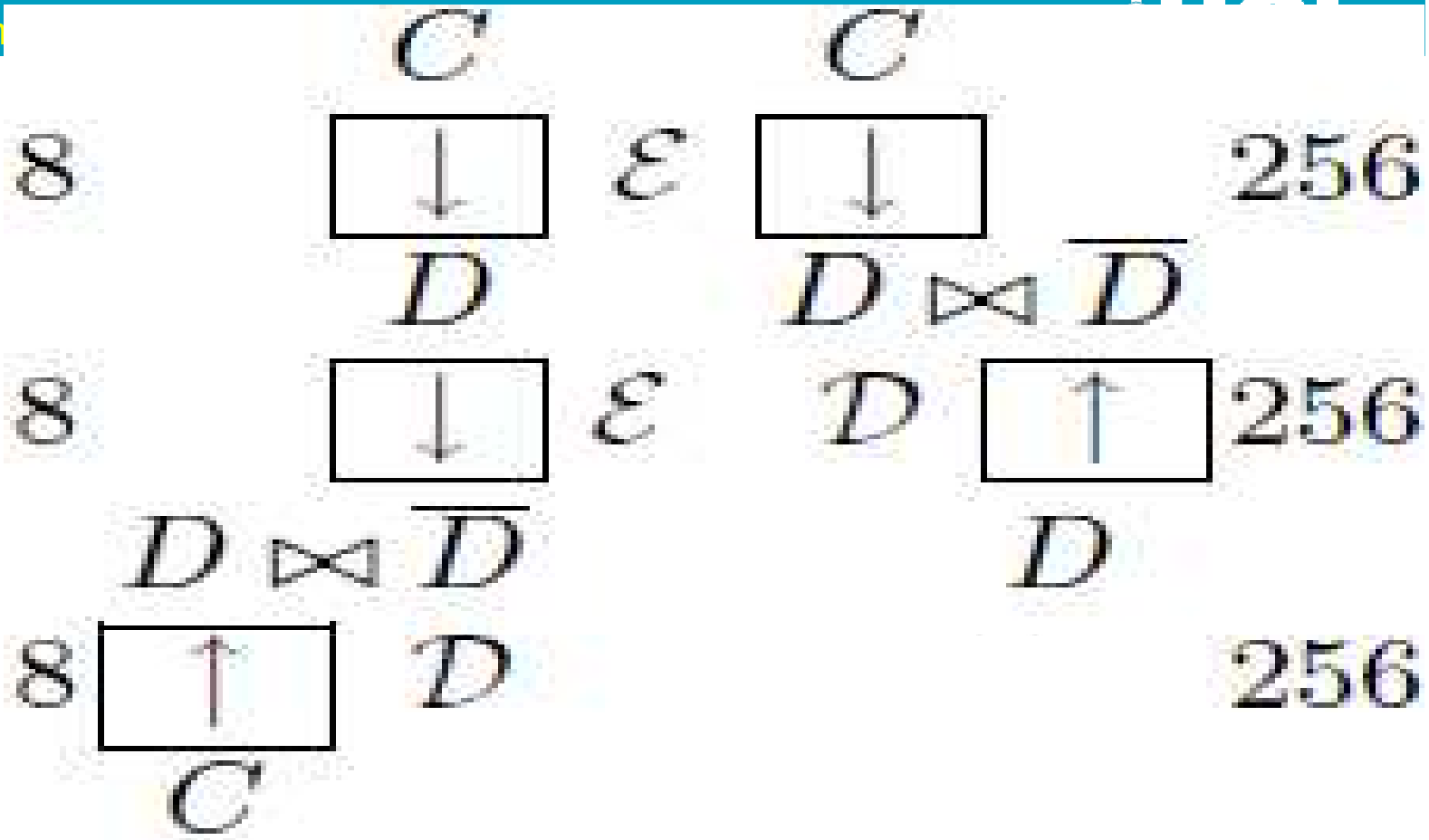


Assumptions

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.

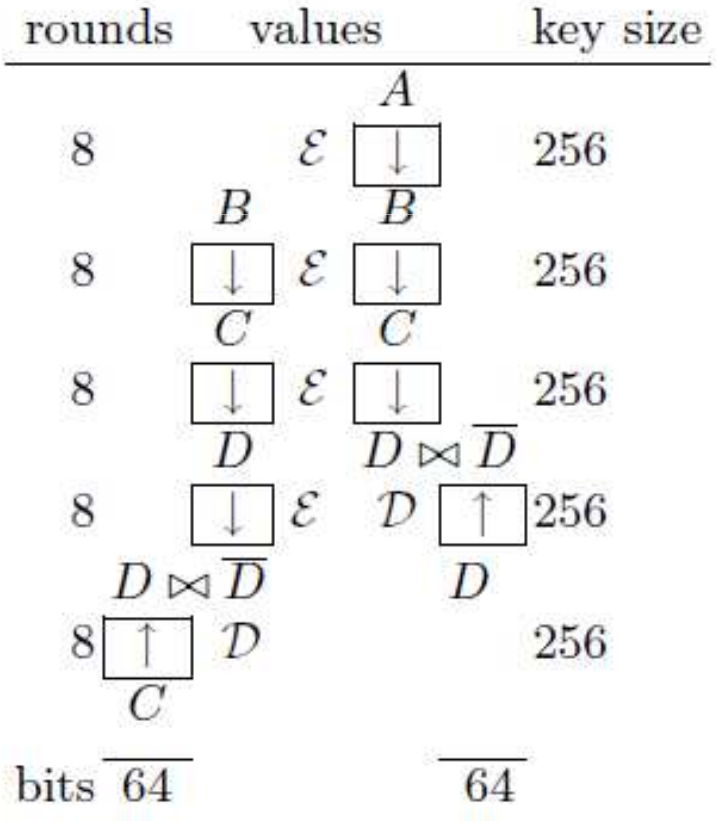
Remark: For the remaining 37 % of keys this attack fails. However many other attacks still work, see [12].

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^{110} GOST computations.

Overall Attack

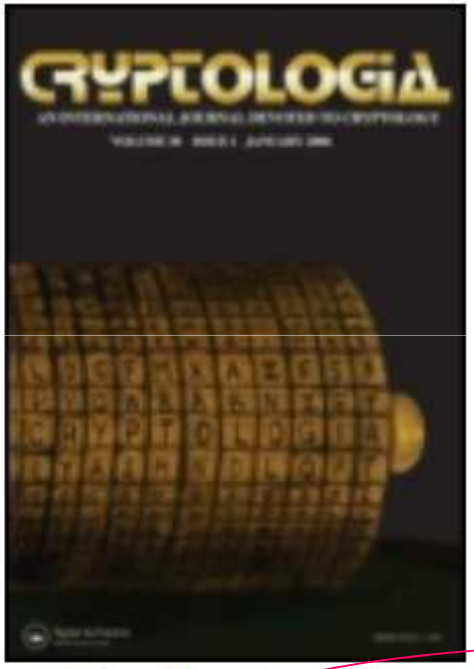
$2^{128+110}$ GOST computations.

2^{17} 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 $\in$ 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.

⇒ For now nothing bad happened, just some bad press.

⇒ Is GOST really broken? Not sure it is.

Science ≠ Politics

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

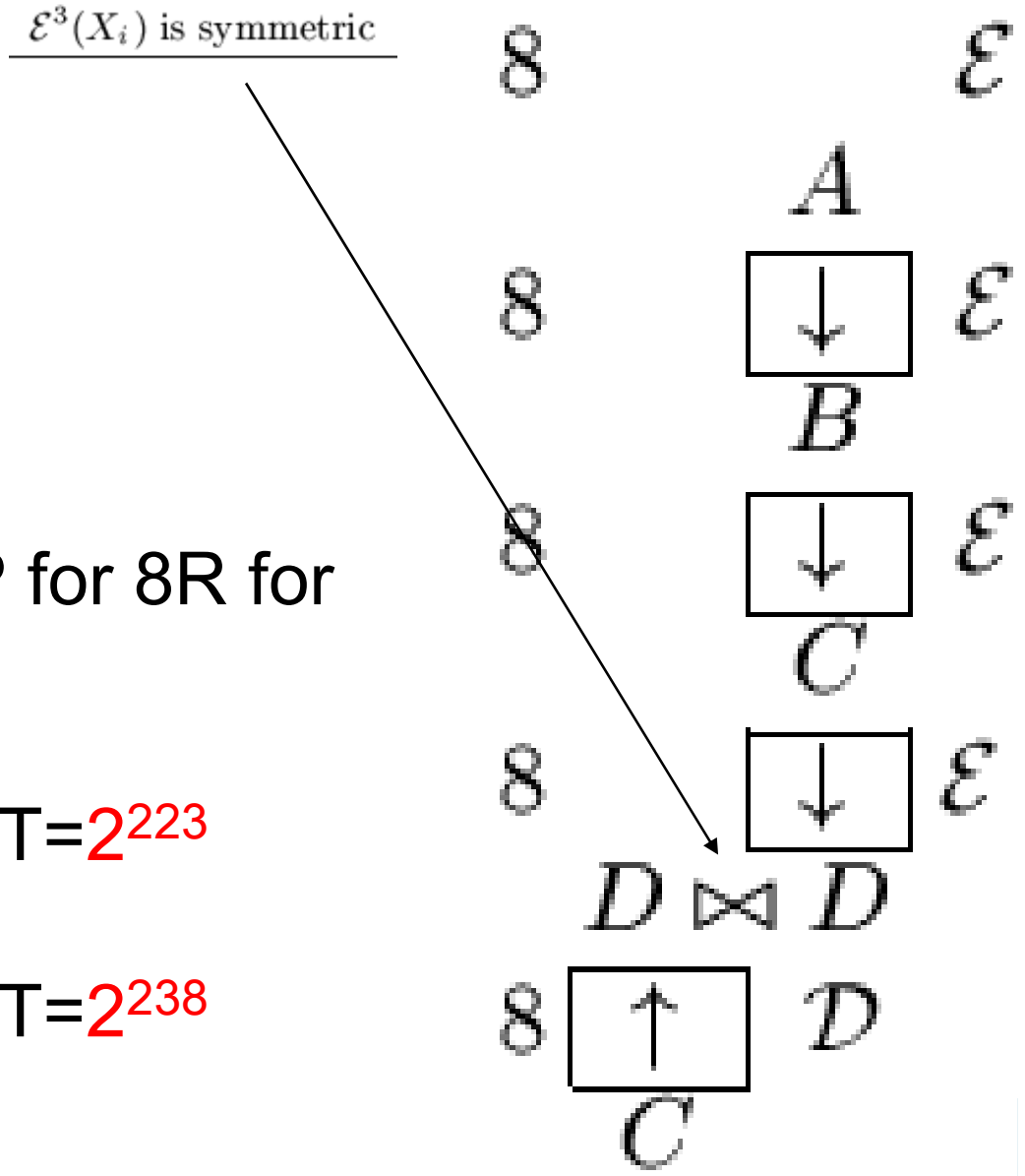
Reflection – Happens 2^{32} Times - KPA

- 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

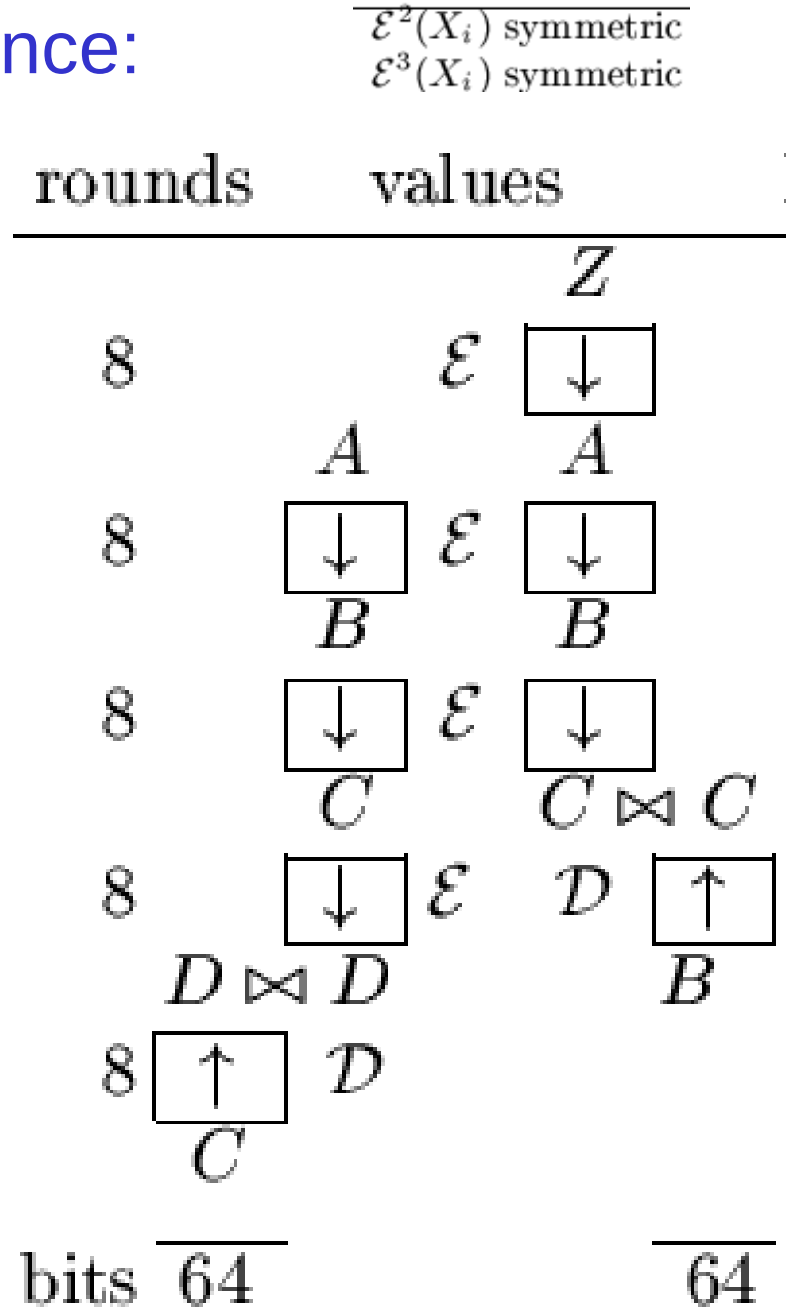
2x Reflection, Happens About Once:

- 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}

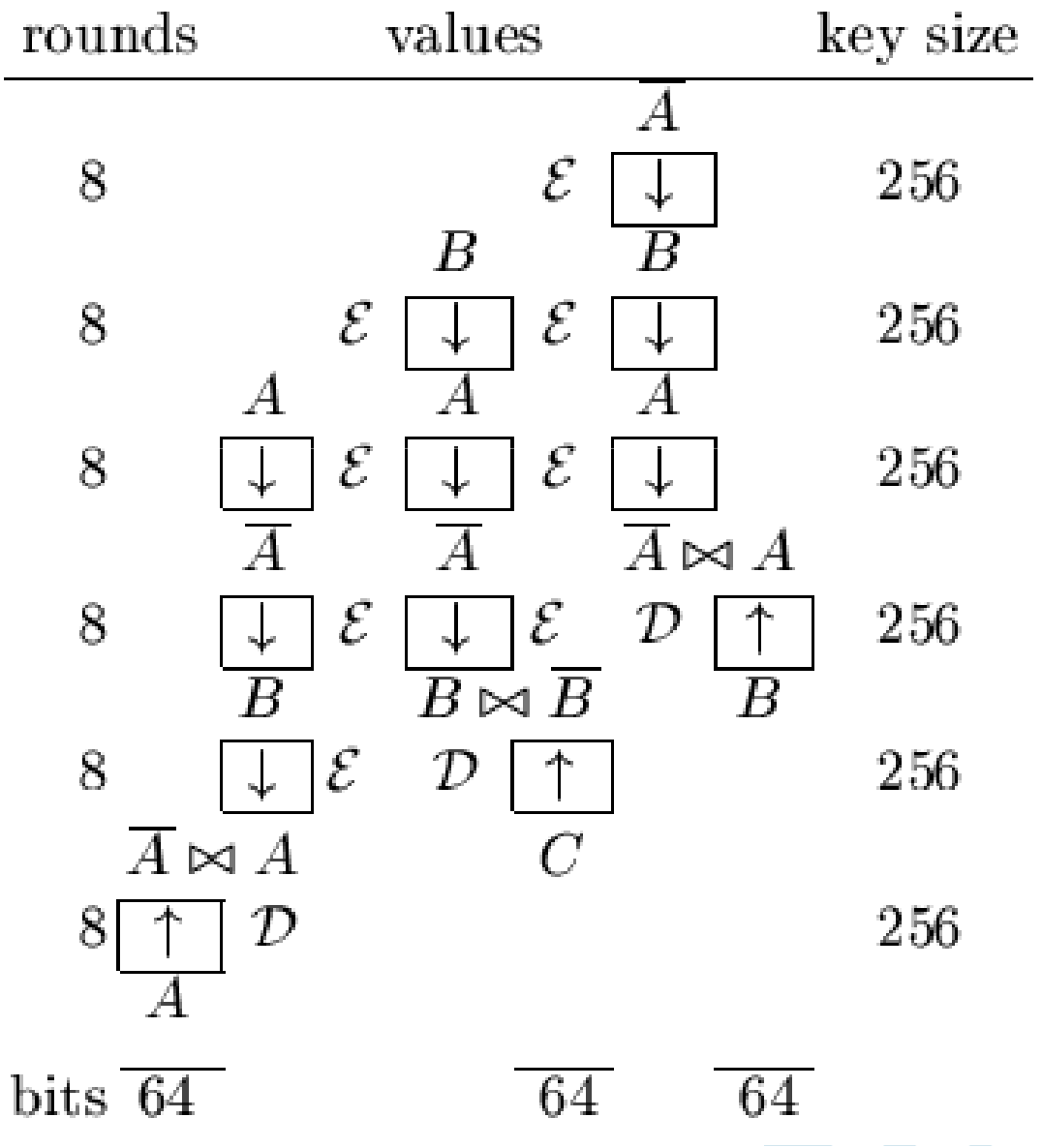
$$\mathcal{E}^2(\overline{A}) = A$$

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

No guessing =>

Very high amplification.

All data obtained nearly “for free”.



7.2. 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.

Combined DC+Algebraic Complexity Reduction

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

rounds	values/differences	key size
	$A \leftarrowtail 80700700\ 80700700 \rightarrowtail B$	
8	$\boxed{\downarrow}\ \mathcal{E}\ \boxed{\downarrow}$	256
	$A \leftarrowtail 80700700\ 80700700 \rightarrowtail B$	
8	$\boxed{\downarrow}\ \mathcal{E}\ \boxed{\downarrow}$	256
	$A \leftarrowtail 80700700\ 80700700 \rightarrowtail B$	
8	$\boxed{\downarrow}\ \mathcal{E}\ \mathcal{E}\ \boxed{\downarrow}$	256
	$A \bowtie A \leftarrowtail 80700700\ 80700700 \rightarrowtail B \bowtie \overline{B}$	
8	$\boxed{\uparrow}\ \mathcal{D}\ \mathcal{D}\ \boxed{\uparrow}$	256
bits	$\frac{A}{64}$ $\frac{C}{64}$	

8. 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!

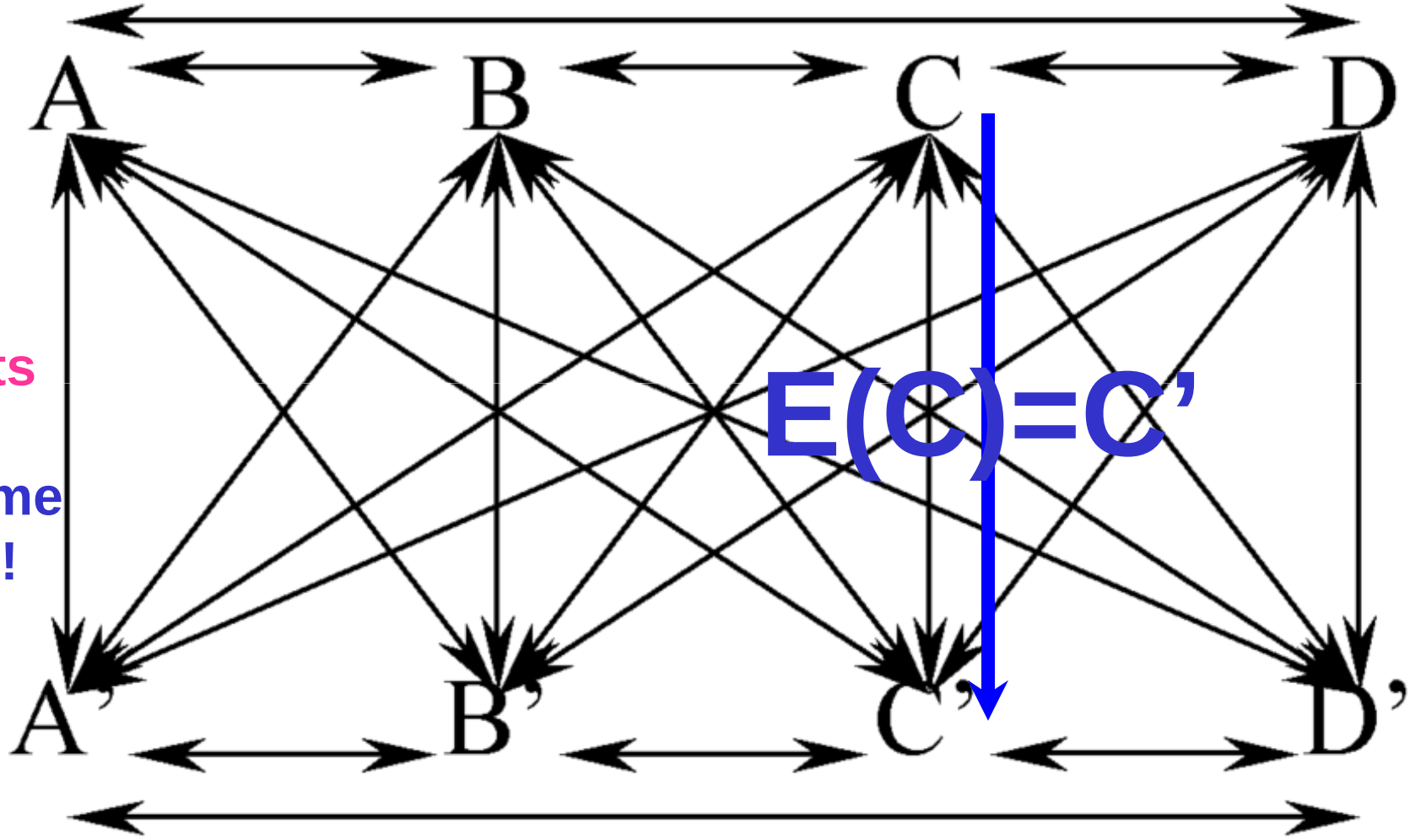


Fig. 18. An approximate fixed point biclique with $k = 4$

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…

8.2. Summary

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 $\geq$	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)

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.

8.3.
Facts or Fictions?

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…