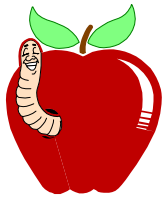
Bugs or Backdoors?

with focus on Older / Industrial / Historical Crypto



Nicolas T. Courtois

University College London, UK

Dr. Nicolas T. Courtois

1. cryptologist and codebreaker

UNIVERSITY CIPHER CHAMPION

March 2013

Cyber Security Challenge UK

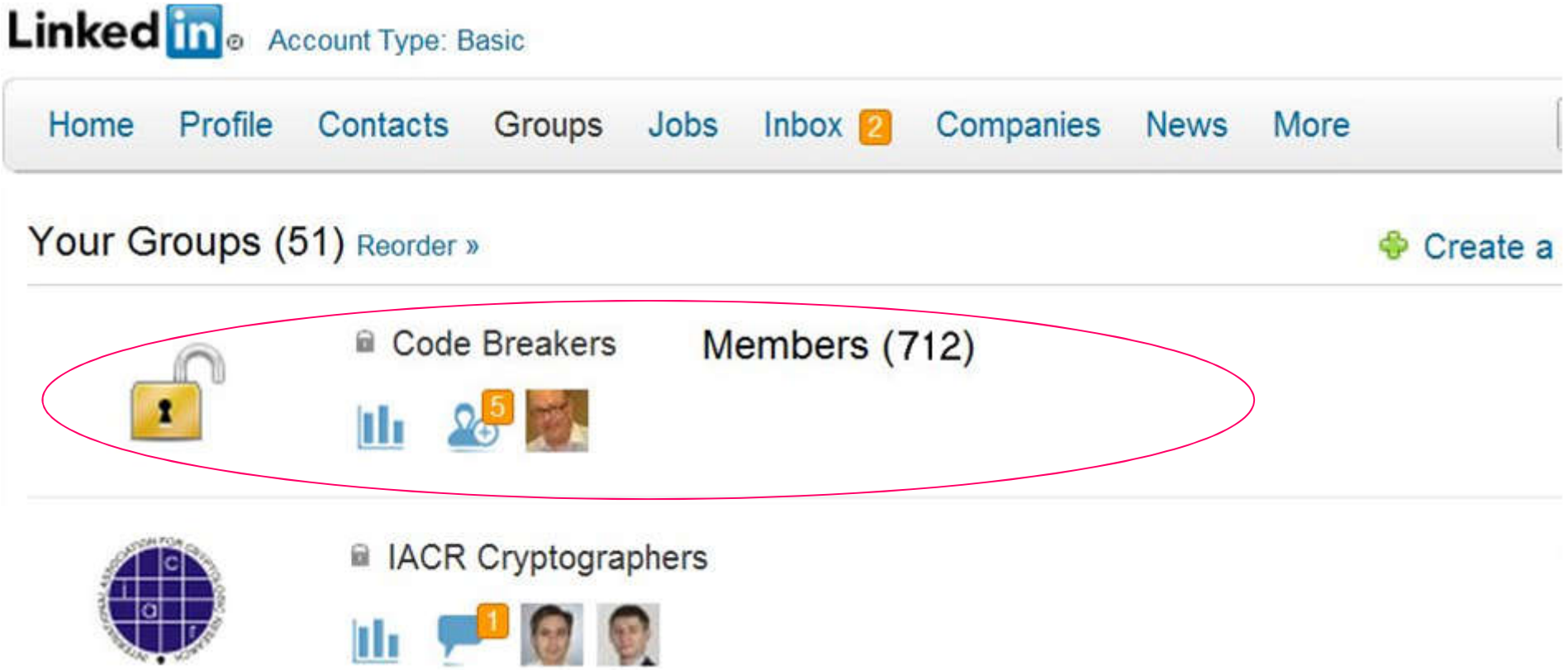
2. payment and smart cards (e.g. bank cards, Oyster cards etc…)

Oyster cracker vows to clone cards

Cloning kit could sell for just £200, says researcher

Robert Blincoe, vnunet.com, 28 Jul 2008

LinkedIn


LinkedIn
Account Type: Basic
Home
Profile
Contacts
Groups
Jobs
Inbox 2
Companies
News
More
Your Groups (51) Reorder »
Create a
Code Breakers
Members (712)
5
IACR Cryptographers
1

My Blog

http://blog.bettercrypto.com

CRYPTANALYSIS

better cryptography, better and faster crypto currencies, cyber security, applied cryptograp

HOME | SEMINARS | EVENTS | TOPICS | RESOURCES | ABOUT

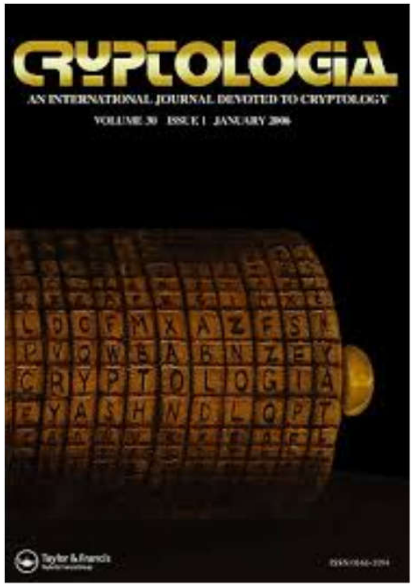
NSA Plans To Retire Current Cryptography Standards

Posted by admin on 15 September 2015, 3:26 pm

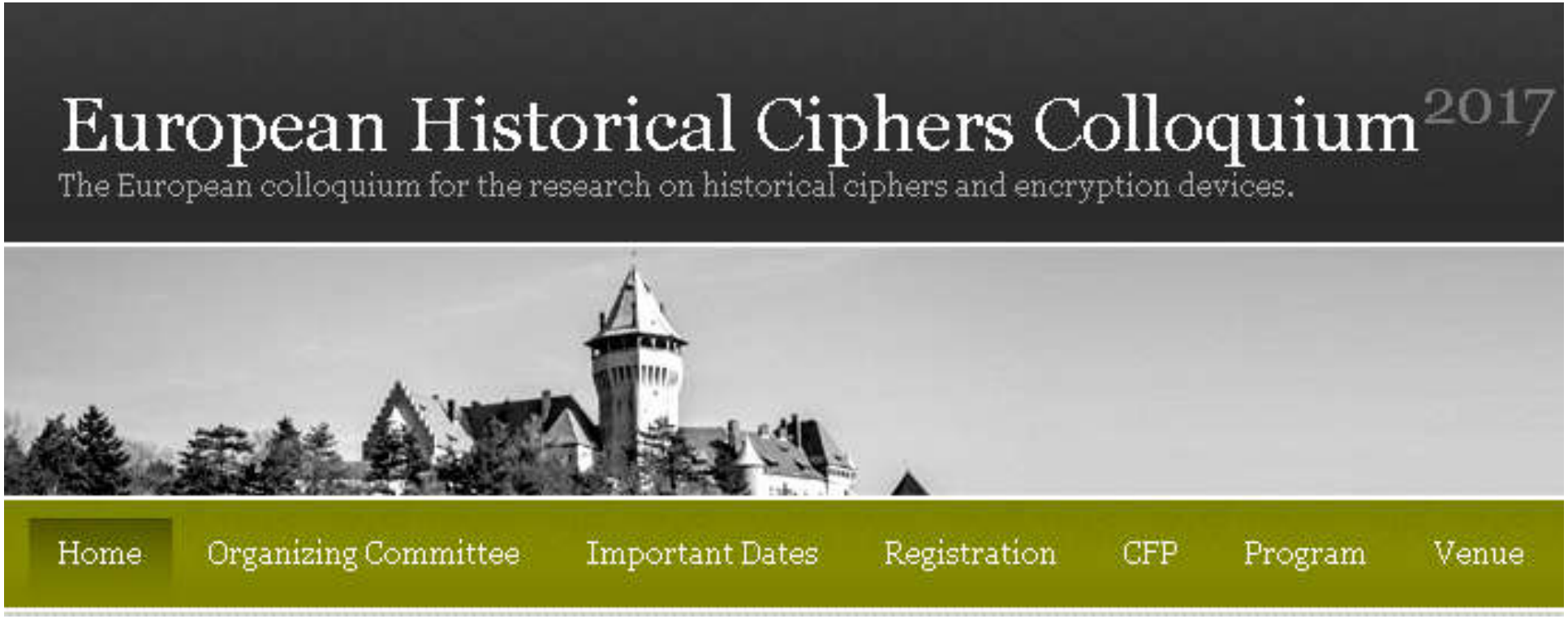
Breaking news:
the cryptography that we all know and use, such AES-128, SHA-1 and SHA-256, RSA/DH, and the most commonly used elliptic curve **P-256** (a.k.a. secp256r1) are NO LONGER wholeheartedly supported by the NSA. In fact most of these, if not all, are **not quite recommended anymore**.

Until now and for the last 10+ years the NSA and the NIST urged everybody to use these things. Now the NSA has a very different message:

Crypto History



Next Euro-HCC

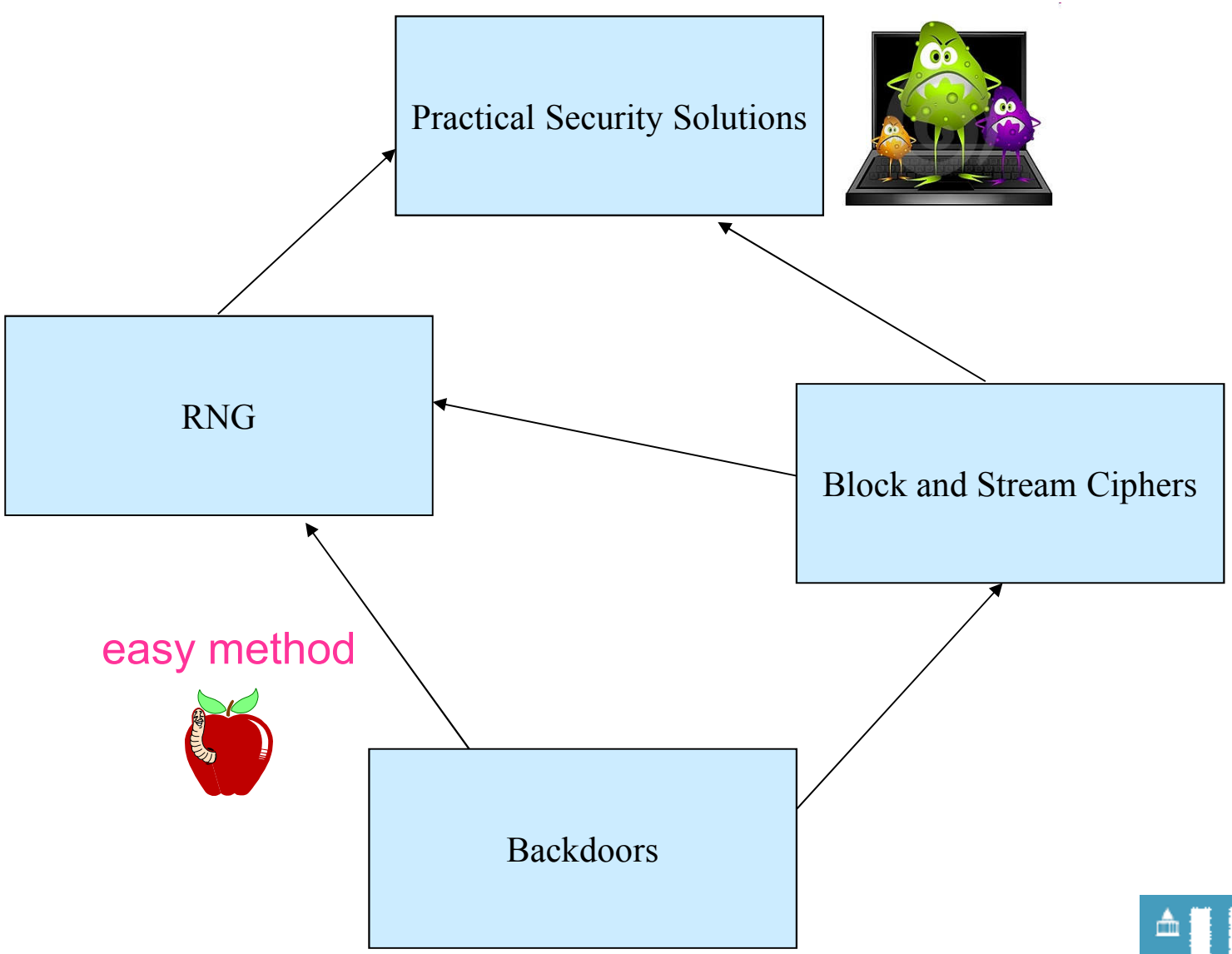


18-19 May, Slovakia

18-19 May Program

Day 1 – 18th May 2017	Day 2 – 19th May 2017
Opening Conference and Welcome K. Nemoga 09:00 - 09:15	**History of public key cryptography and RSA – Session Chair: B. Esslinger** J.-J. Quisquater 09:00-10:00
The 'Gustave Bertrand' files – Session Chair: N. Courtois D. Turing 09:15 - 9:45	
Session 1 – Session Chair: G.F. Strasser Slot 1: 09:45 - 10:15: G. Lasry - The Hagelin Cryptosystems - Historical and Modern Cryptanalysis **Coffee Break 10:15 - 10:45** Slot 2: 10:45 - 11:15: N. Kopal - A General Solution for the M-94 Slot 3: 11:15 - 11:45: J. Kollár - Determining the text reading direction of an unknown text Slot 4: 11:45 - 12:15: B. Esslinger - Automated Cryptanalysis of Classical Ciphers	**Session 3 – Session Chair: K. Schmeh** Slot 9: 10:00 - 10:30: P. Bonavoglia - How I decrypted Pietro Giannone's last poem **Coffee Break 10:30 - 11:00** Slot 10: 11:00 - 11:30: G.F. Strasser - Wolfenbüttel, a Minor German Duchy but a Major Center of Cryptology in the Early Modern Period Slot 11: 11:30 - 12:00: S. Porubsky - STP cipher of the Czechoslovak Ministry of Defence in London during WWII Slot 12: 12:00 - 12:30: M. Grajek - Interrogation at Eisenberg Castle - How two Polish officers saved the Ultra secret just before Overlord
Lunch 12:15 - 13:30	
Session 2 – Session Chair: D. Turing Slot 5: 13:30 - 14:00: K. Schmeh - German Spy Ciphers of World War II Slot 6: 14:00 - 14:30: C. Taaks - The Early Times of the Enigma – Political, Economic and Military **Coffee Break 14:30 - 15:00** Slot 7: 15:00 - 15:30: P. Guillot - The priceless gift - The Polish cryptanalysis of Enigma Slot 8: 15:30 - 16:00: M-J. Durand-Richard - Cryptology at Bletchley Park (1939-1945)	**Closing Remarks** 12:30 - 12:45 **Lunch and/or departure** 12:45 - 14:00

Topics


Practical Security Solutions
RNG
Block and Stream Ciphers
Backdoors
easy method

Bad Randoms – 1930s – Enigma Message Keys

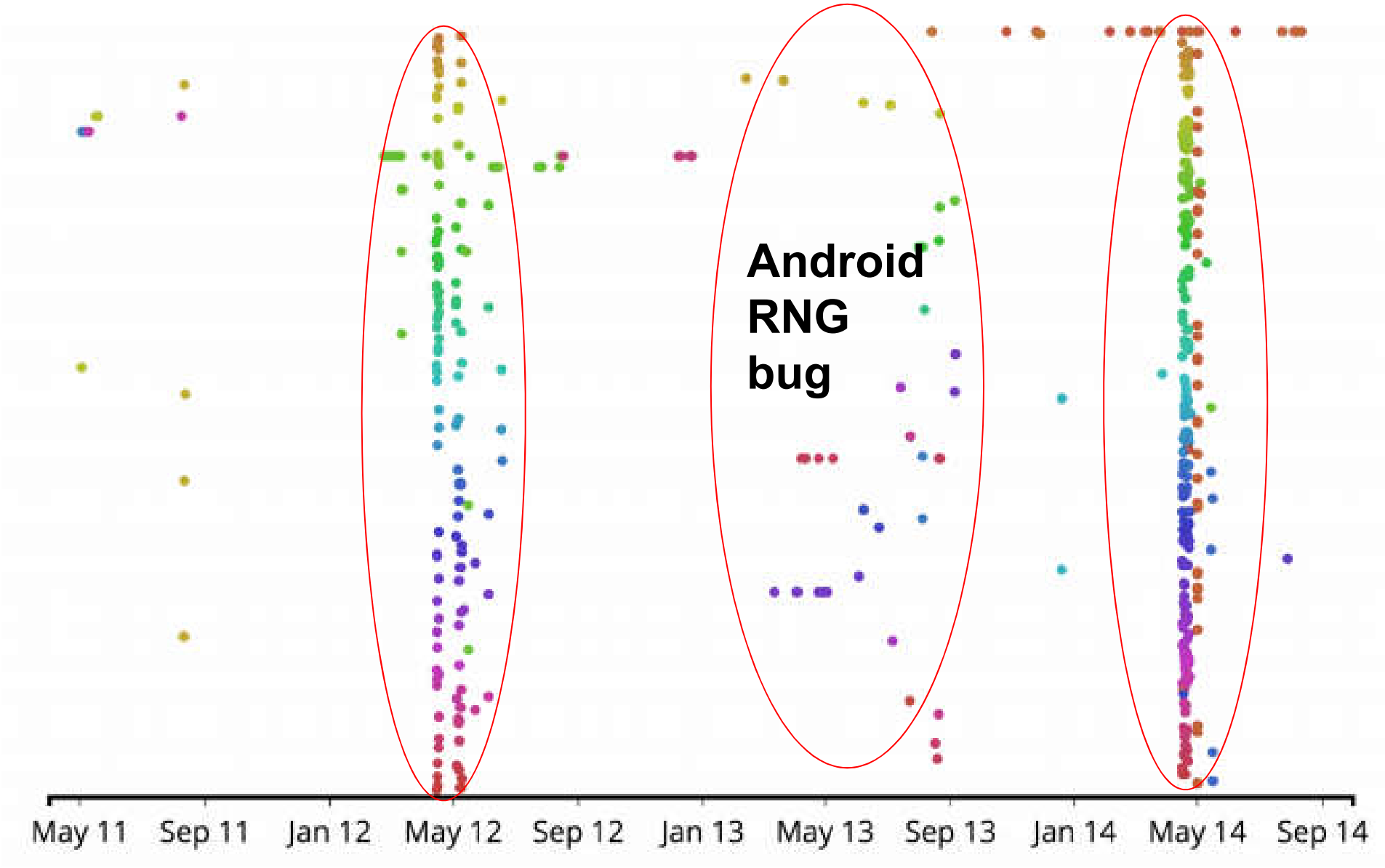
(should be 3 random letters)

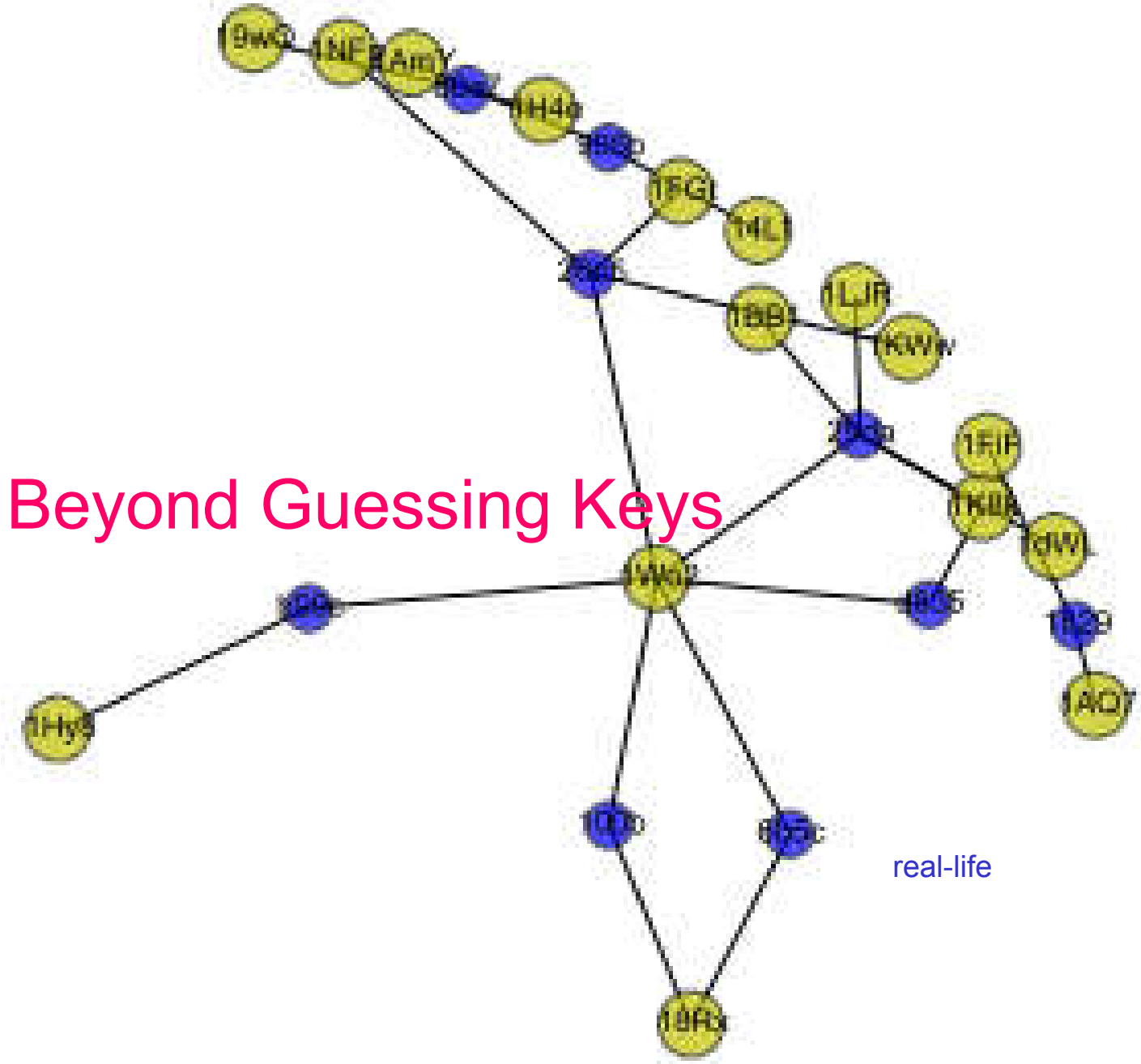
~~AAA~~

~~XYZ~~

Operators always found a way to «degrade » their security

Bitcoin – cf. Nadia Talk



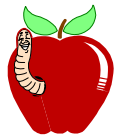

Beyond Guessing Keys
real-life

This talk

- Bad RNG – yes but too easy.

This talk:

- Better / less obvious ways to backdoor!



  - Sophisticated attacks which combine several vulnerabilities.
  - How to backdoor symmetric encryption?

Birth of Modern Crypto

1960s – NATO cipher competition

Actes du septième Colloque sur l'Histoire de l'Informatique et des Transmissions 95

Histoire de la machine Myosotis [2004]

Xavier Ameil, Jean-Pierre Vasseur et Gilles Ruggiu

Association des Réservistes du Chiffre et de la Sécurité des Informations

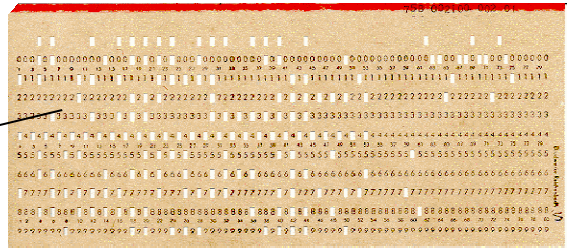
"tapeless and rotorless" => semi-conductor electronic, high EM security

- large period, non-linearity / removing the correlations (p.108)

"…certainement la meilleure machine cryptographique de son époque…"

??

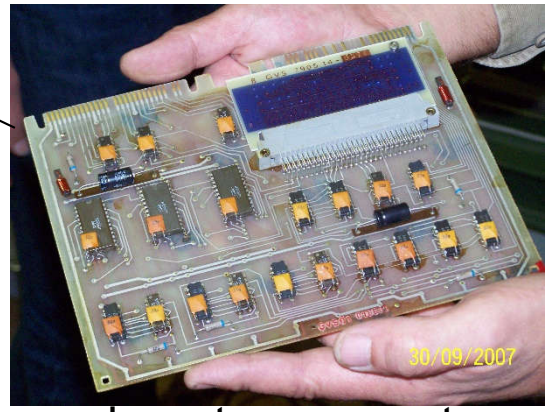
East German SKS V/1 and T-310



240 bits

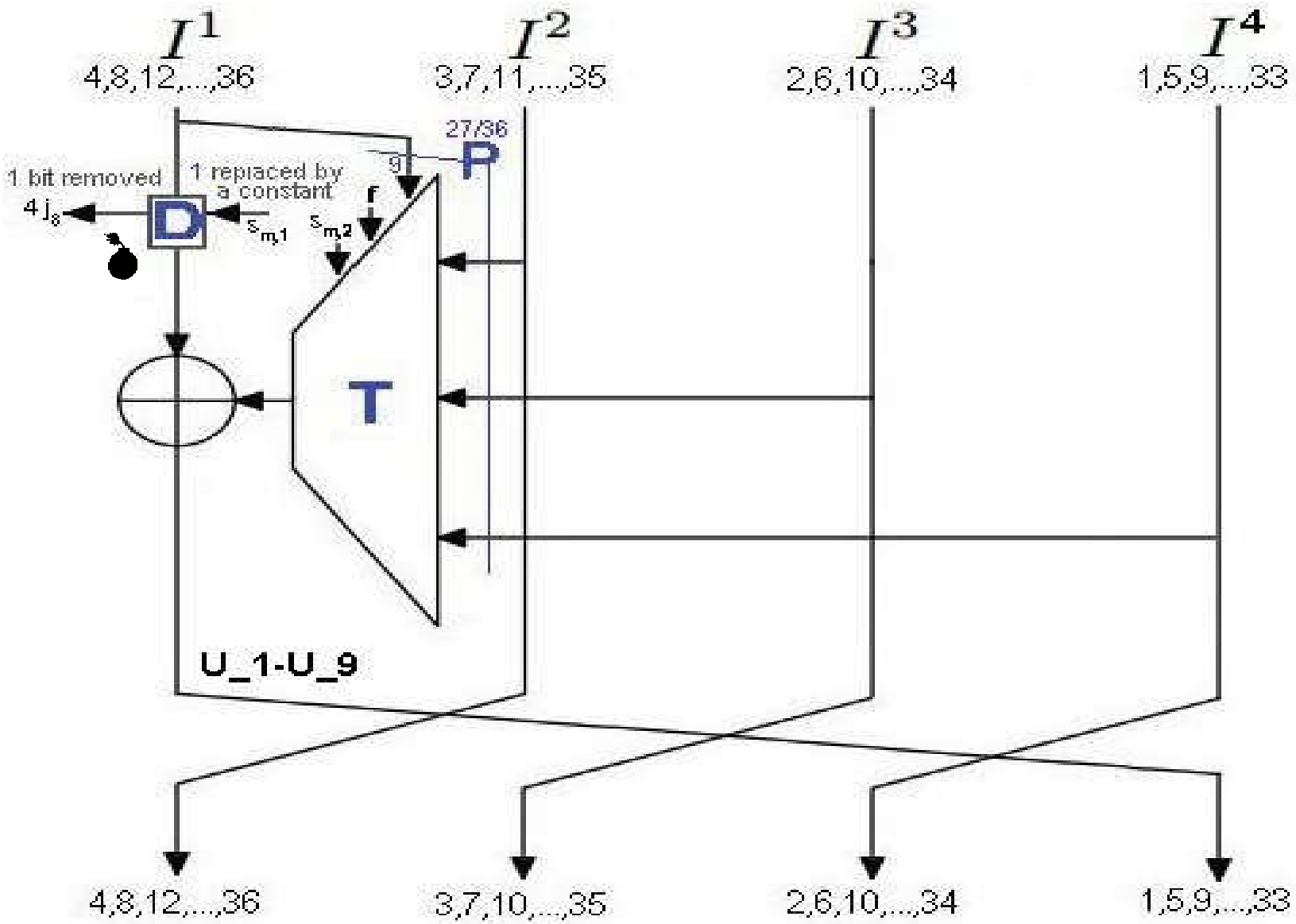
"quasi-absolute security"
[1973-1990]

has a physical RNG=>IV



long-term secret
90 bits only!

Contracting Feistel [before 1975]



How to Backdoor T-310 [to appear in 2017]

omit just 1 out of 40 conditions:

D and P are injective

$P(3) = 33, P(7) = 5, P(9) = 9, P(15) = 21, P(18) = 25, P(24) = 29$

Let $W = \{5, 9, 21, 25, 29, 33\}$

$\forall_{1 \geq i \geq 9} D(i) \notin W$

$\alpha \notin W$

Let $T = (\{0, 1, \ldots, 12\} \backslash W) \cap (\{P(1), P(2), \ldots, P(24)\} \cup \{D(4), D(5), \ldots, D(9)\} \cup \{\alpha\})$

Let $U = (\{13, \ldots, 36\} \backslash W) \cap (\{P(26), P(27)\} \cup \{D(1), D(2), D(3)\})$

$|T \backslash \{P(25)\}| + |U \backslash \{P(25)\}| \leq 12$

$A = \{D(1), D(2), D(3), D(4), D(5), D(6), D(7), D(8), D(9)\} \cup \{P(6), P(13), P(20), P(27)\}$

$A_1 = \{D(1), D(2)\} \cup \{P(27)\}$

$A_2 = \{D(3), D(4)\} \cup \{P(20)\}$

$A_3 = \{D(5), D(6)\} \cup \{P(13)\}$

$A_4 = \{D(7), D(8)\} \cup \{P(6)\}$

$\forall (i, j) \in \{1, \ldots, 27\} \times \{1, \ldots, 9\} : P_i \neq D_j$

$\exists j_1 \in \{1, \ldots, 7\} : D_{j_1} = 0$

$\{D(8), D(9)\} \subset \{4, 8, \ldots, 36\} \subset A$

$\forall (i, j) \in \overline{1,27} \times \overline{1,9} : P_i \neq D_j$

$\exists j_1 \in \overline{1,7} : D_{j_1} = 0$

$\{D_8, D_9\} \subset \{4, 8, \ldots, 36\} \subset A$

$\exists (j_2, j_3) \in (\{j \in \overline{1,4} | D_j ? \notin A_j\})^2 \wedge$

$\exists (j_4, j_5) \in (\overline{1,4} \setminus \{j_1, 2j_2 - 1, 2j_2\}) \times (\overline{5,8} \setminus \{j_1, 2j_2 - 1, 2j_2\}) \wedge$

$\exists j_6 \in \overline{1,9} \setminus \{j_1, 2j_2 - 1, 2j_2, j_4, j_5\} :$

$j_2 \neq j_3 \wedge \{4j_4, 4j_5\} \subset A_{j_2} \wedge$

$A_{j_2} \cap (\overline{4j_1 - 3, 4j_1} \cup \overline{4j_6 - 3, 4j_6}) \neq \emptyset \wedge$

$\{8j_2 - 5, 8j_2\} \subset A_{j_3} \wedge A_{j_3} \cap (\overline{4j_1 - 3, 4j_1} \cup \overline{4j_6 - 3, 4j_6}) \neq \emptyset;$

$\{D(9)\} \setminus (\overline{33,36} \cup \{0\}) \neq \emptyset$

$\{D(8), D(9), P(1), P(2), \ldots, P(5)\} \setminus (\overline{29,32} \cup \{0\}) \neq \emptyset$

$\{D(7), D(8), P(1), P(2), \ldots, P(6)\} \setminus (\overline{25,32} \cup \{0\}) \neq \emptyset$

$\{D(7), D(9), P(1), P(2), \ldots, P(6)\} \setminus (\overline{25,28} \cup \overline{33,36} \cup \{0\}) \neq \emptyset$

$\{D(6), D(7), D(8), D(9), P(1), P(2), \ldots, P(12)\} \setminus (\overline{21,36} \cup \{0\}) \neq \emptyset$

$\{D(5), D(7), D(8), D(9), P(1), P(2), \ldots, P(13)\} \setminus (\overline{17,20} \cup \overline{25,36} \cup \{0\}) \neq \emptyset$

$\{D(7), D(8), D(9), P(1), P(2), \ldots, P(6)\} \setminus (\overline{25,36} \cup \{0\}) \neq \emptyset$

$\{D(5), D(6), D(8), D(9), P(1), P(2), \ldots, P(13)\} \setminus (\overline{17,24} \cup \overline{29,36} \cup \{0\}) \neq \emptyset$

$\{D(5), D(6), D(7), D(9), P(1), P(2), \ldots, P(13)\} \setminus (\overline{17,28} \cup \overline{33,36} \cup \{0\}) \neq \emptyset$

$\{D(5), D(6), D(7), D(8), P(1), P(2), \ldots, P(13)\} \setminus (\overline{17,32} \cup \{0\}) \neq \emptyset$

$\{D(5), D(6), D(7), D(8), D(9), P(1), P(2), \ldots, P(13)\} \setminus (\overline{17,36} \cup \{0\}) \neq \emptyset$

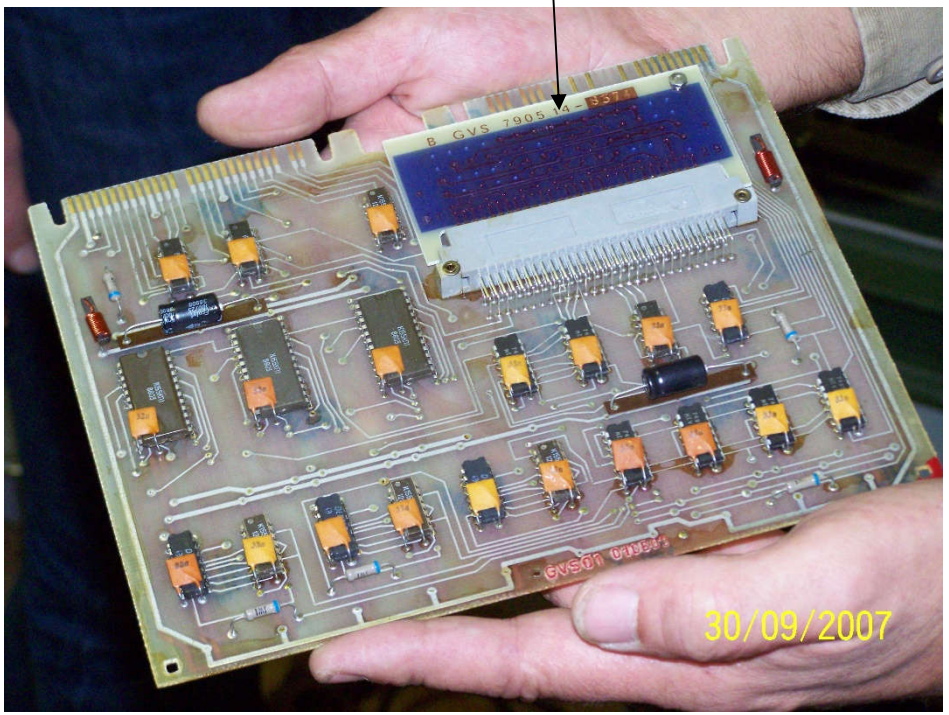
$\{D(4), D(5), \ldots, D(9), P(1), P(2), \ldots, P(19)\} \setminus (\overline{13,36} \cup \{0\}) \neq \emptyset$

$\{D(3), D(4), \ldots, D(9), P(1), P(2), \ldots, P(20)\} \setminus (\overline{9,36} \cup \{0\}) \neq \emptyset$

plus the "Matrix *rank* = 9 condition" M_9 defined in Section D.4 below.

ciphertext-only

bad long-term key



bug or backdoor?

False Backdoors = def =

strong properties of ciphers/systems/RNGs which exist for NO apparent reason or/and which are clearly harmful/counterproductive.

- in some cases a really good attack was never found!
- or maybe we just discovered ½ of what we need to uncover?

Mystery Paper - Shamir 1985

On the Security of DES

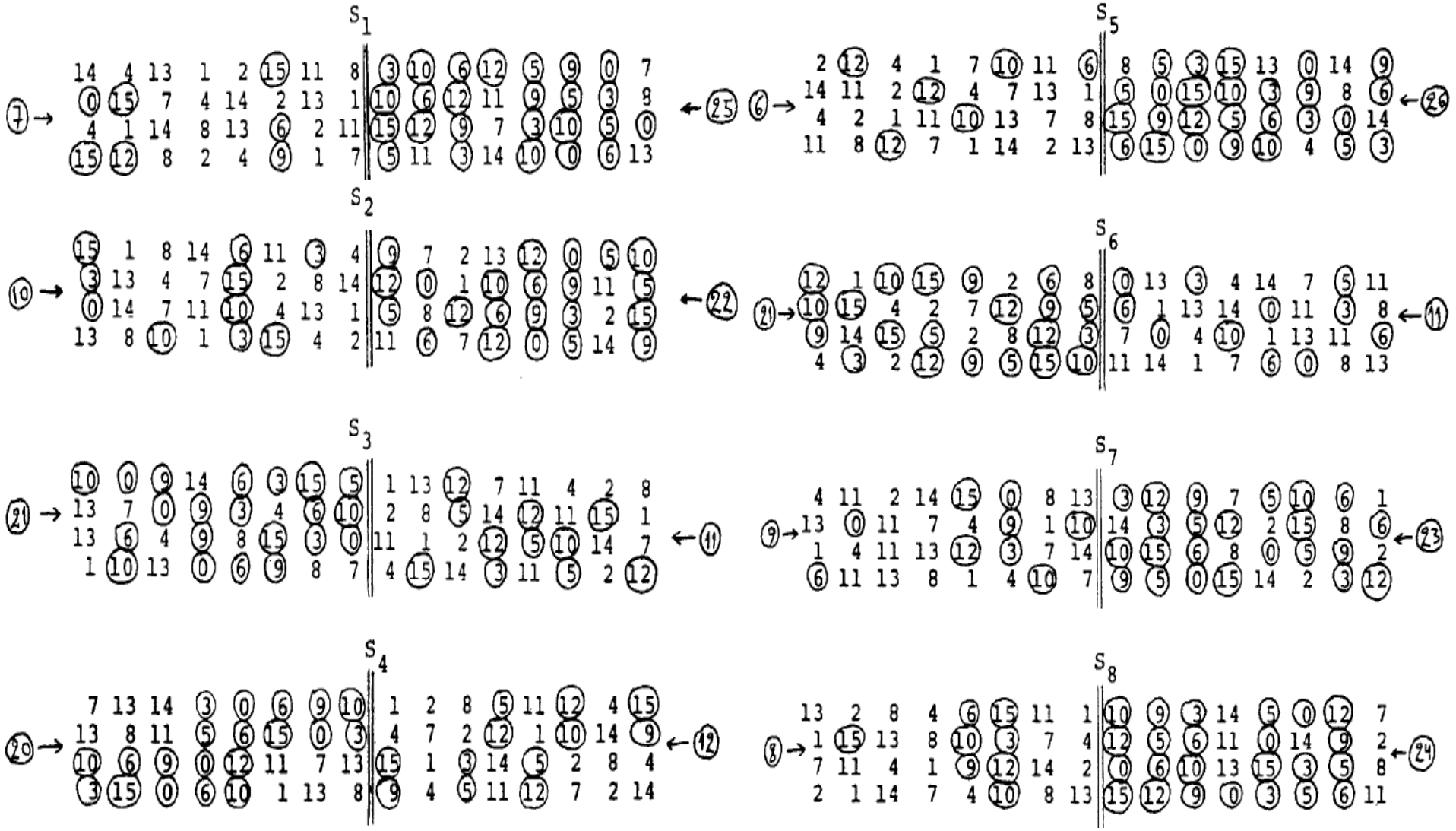
Adi Shamir
Applied Mathematics
The Weizmann Institute
Rehovot, Israel
(abstract)

The purpose of this note is to describe some anomalies found in the structure of the S-boxes in the Data Encryption Standard. These anomalies are potentially dangerous, but so far they have not led to any successful cryptanalytic attack.

Mystery thing.

Related to LC published 8 years later.

** Shamir 1985



Shamir 1985

On the Security of DES

Adi Shamir
Applied Mathematics
The Weizmann Institute
Rehovot, Israel
(abstract)

$x_2 \approx y_1 \oplus y_2 \oplus y_3 \oplus y_4$.

Common to all S-boxes !!!!

Mystery never explained, super strong pty,

We found more such properties [Courtois, Goubin, Castagnos 2003/184]

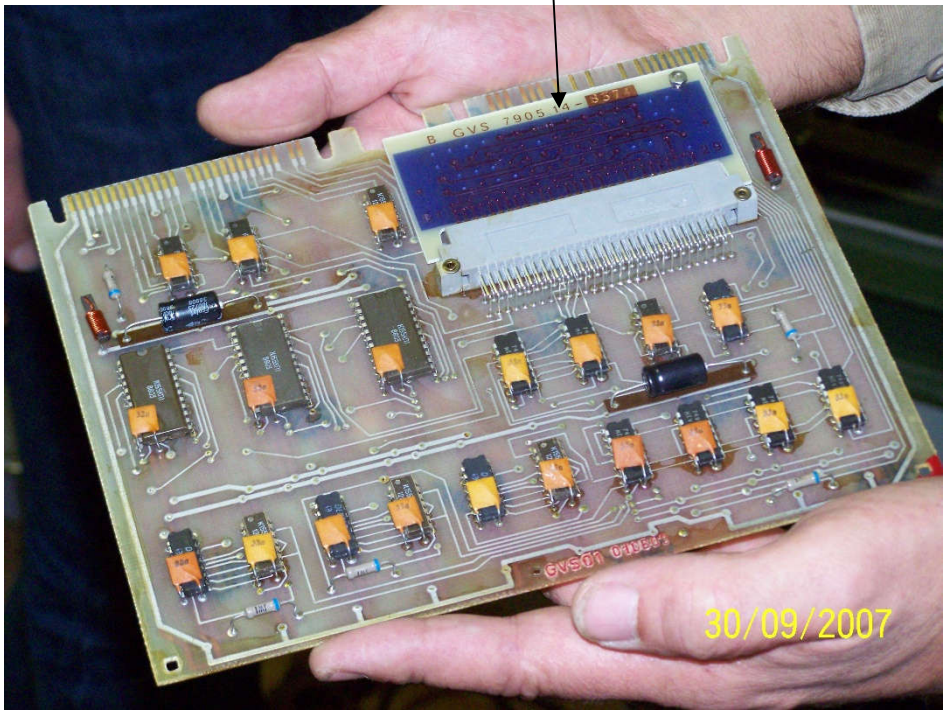
Another Method to Backdoor T-310

1,3,5 => 1,3,5

P=1

703
P=7,14,33,23,18,36,5,2,9,
16,30,12,32,26,21,1,13,25,
20,8,24,15,22,29,10,28,6
D=0,4,24,12,16,32,28,36,20

bad long-term key



MiFare Classic Crypto-1 Cipher
or The Tale of 4 “Backdoors”

Parity Attacks

Backdoor 1: The card does encrypt data with redundancy.

One should never do that.

- more costly
- weaker
  - and even weaker with a stream cipher:

    Ciphertext Only attack (weak)=>

    gives (small weight) LINEAR equations on the keystream (very strong)

Same problem: GSM

Cf. [Biham-Barkan-Keller: Instant Ciphertext-Only Cryptanalysis of GSM.. Crypto'03 and JoC'08]

Same Problem – Enigma WW2

ciphertext

plaintext

Double Encryption Method – Big Mistakes

15 Sept 1938 - 1 May 1940 [sometimes also used later, e.g. Norway, Malta 1942]

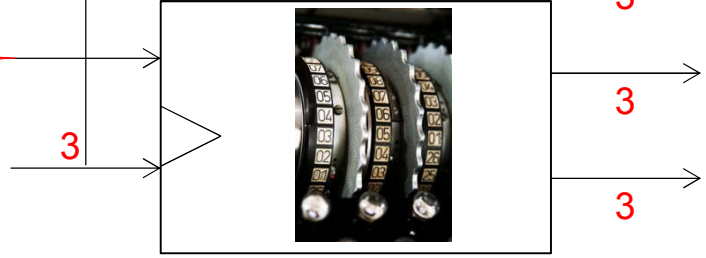
3 digit « random »
message key

repeat twice

3 3

daily settings:
-rotors I III IV
-ring settings
-random start

«random IV »



only 6 digits with the same random start position

9-digit header

Conjugation

"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

$S^{-1} \circ R_1 \circ R_4 \circ S$ has a fixed point

<=>

$R_1 \circ R_4$ has a fixed point

Pty independent on stecker!

Zygalski "Netz" Attack on Enigma

fixed points for $R_1 \circ R_4$

Stacking them allowed to determine the key uniquely…

Zygalski

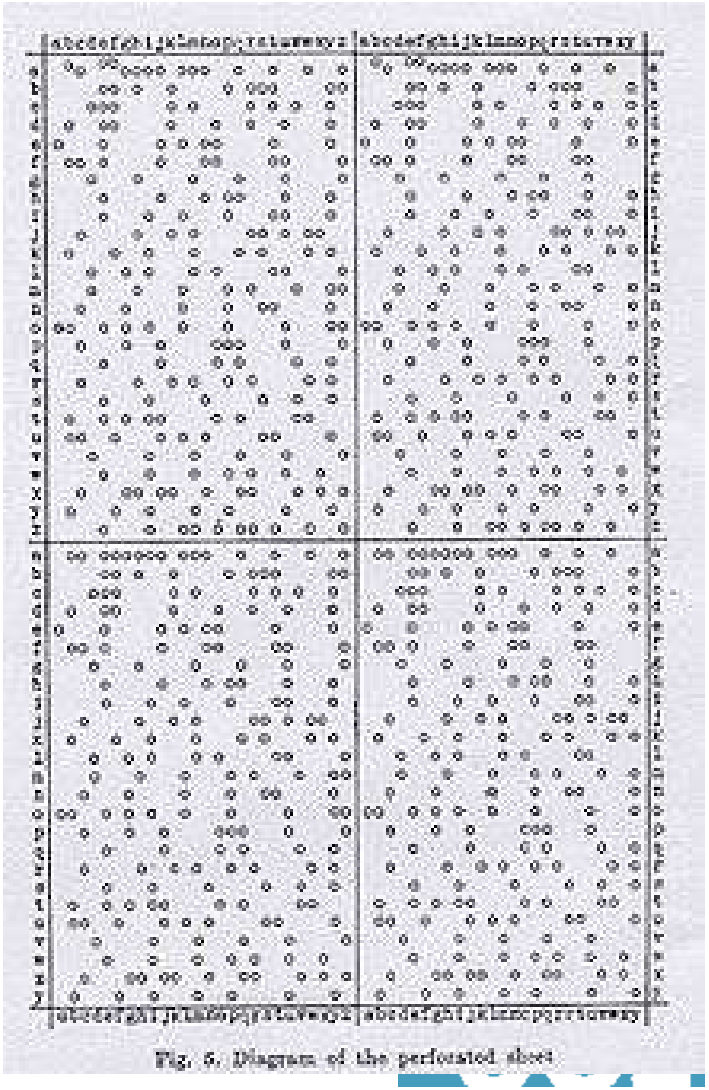


Fig. 6. Diagram of the perforated sheet

attributed by Turing to himself(!) "Turing sheets"

The truth:
=>panic at Bletchley Park: no single message broken
=> chief UK cryptologist (Dilly) wrote a letter saying that he will quit if they do not let Turing travel to France
=>delivered by Turing in person during his visit to France 17 Jan 1940

Backdoor 2: A Bug in MiFare Classic

Discovered accidentally.

- sometimes, under certain conditions, the card outputs a mysterious 4 bits…
- given the fact that many RFID readers are not 100 % reliable, it is easy to overlook it

Then one can guess how it works…

- what are these conditions?,
- can I predict when this will happen?

Parity Weakness…

- Parity bit computed over the plaintext and is encrypted using the same bit as the next plaintext bit
- If all 8 parity bits are correct but the answer is wrong, the tag responds with the 4 bit error code 0x5 encrypted.

$$p_j := n_{T,8j} \oplus n_{T,8j+1} \oplus \cdots \oplus n_{T,8j+7} \oplus 1$$
$$p_{j+4} := n_{R,8j} \oplus n_{R,8j+1} \oplus \cdots \oplus n_{R,8j+7} \oplus 1$$
$$p_{j+8} := a_{R,8j} \oplus a_{R,8j+1} \oplus \cdots \oplus a_{R,8j+7} \oplus 1$$
$$\forall j \in [0, 3]$$

and the encryptions $\{p_j\}$ of these by

$$\{p_j\} := p_j \oplus b_{8+8j} \qquad \forall j \in [0, 11].$$

The Bug?

Or maybe a backdoor?

- Stop pretending that everything happens by accident.
- We need to assume the worst scenario and examine the consequences:
  - Smart card companies are in the position to embed backdoors in products and these will NOT be found for many many years…

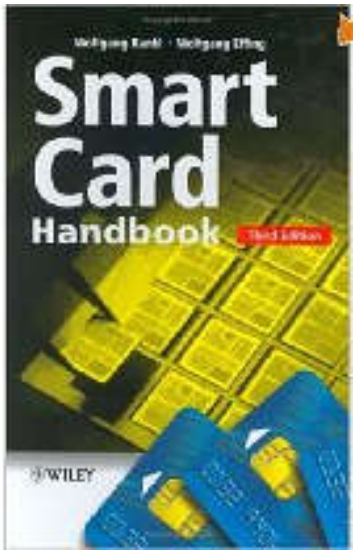
Secure Hardware Dev. Management

[In smart cards] one design criterion differs from the criteria used for standard chips but is nonetheless very important is that absolutely no undocumented mechanisms or functions must be present in the chip ('that's note a bug, that's a feature').

Since they are not documented, they can be unintentionally overlooked during the hardware evaluation and possibly be used later for attacks.

The use of such undocumented features is thus strictly prohibited [...]

[pages 518-519 in the Smart Card handbook
by Wolfgang Rankl and Wolfgang Effing,
1088 pages, Wiley, absolute reference in the industry]



Backdoor 3 - Waste of Silicon

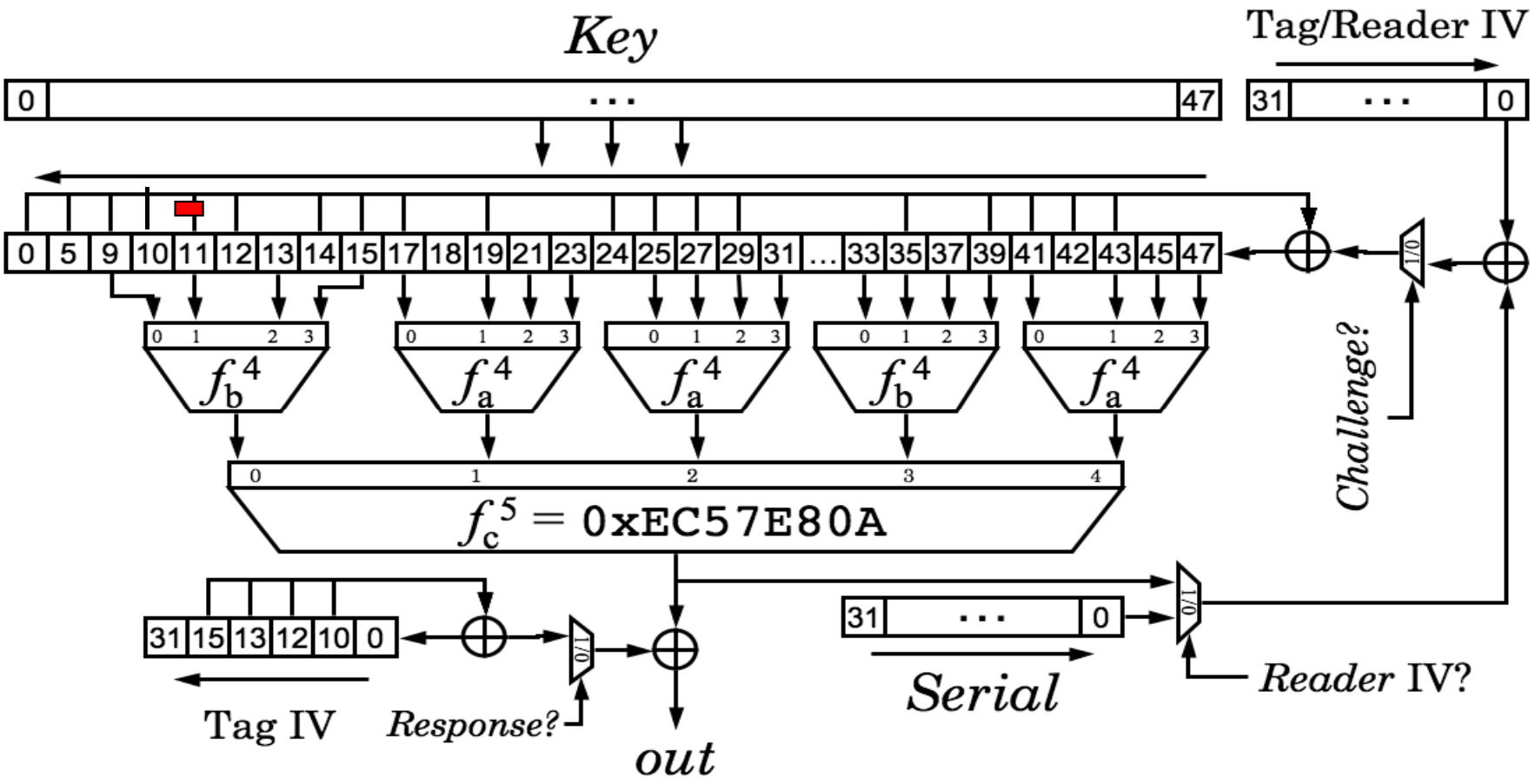
Even a hardware or software designer would NOT notice how weak the cipher is.

Identical Boolean functions are implemented differently. 

Camouflage?

Due to a combination with another terrible weakness half of the silicon is wasted…

Crypto1 Cipher



$f_a^4 = 0x9E98 = (a+b)(c+1)(a+d)+(b+1)c+a$

$f_b^4 = 0xB48E = (a+c)(a+b+d)+(a+b)cd+b$

Tag IV ⊕ Serial is loaded first, then Reader IV ⊕ NFSR

Waste of Silicon

Internal bits are computed 2-3 times.

One could save half of the gates!

“Courtois Dark Side” Attack on MiFare Classic

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

It is a multiple differential attack.

Form of multiple “self-similarity” as well..

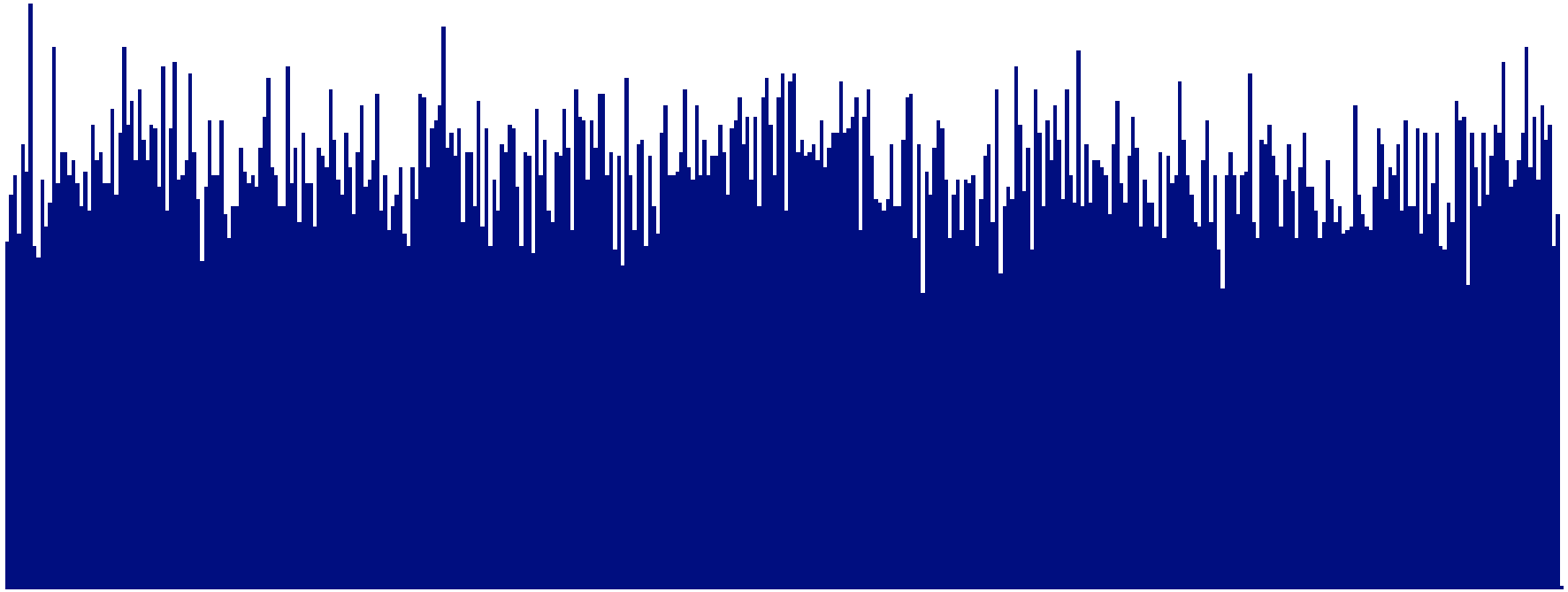
I exhibit a differential that

- holds simultaneously for 256 differentials this works with probability of about 1/17.
- for 8 differentials the probability is about 0.75 (!!).

Both are differences on 51 bits of the state of the cipher.

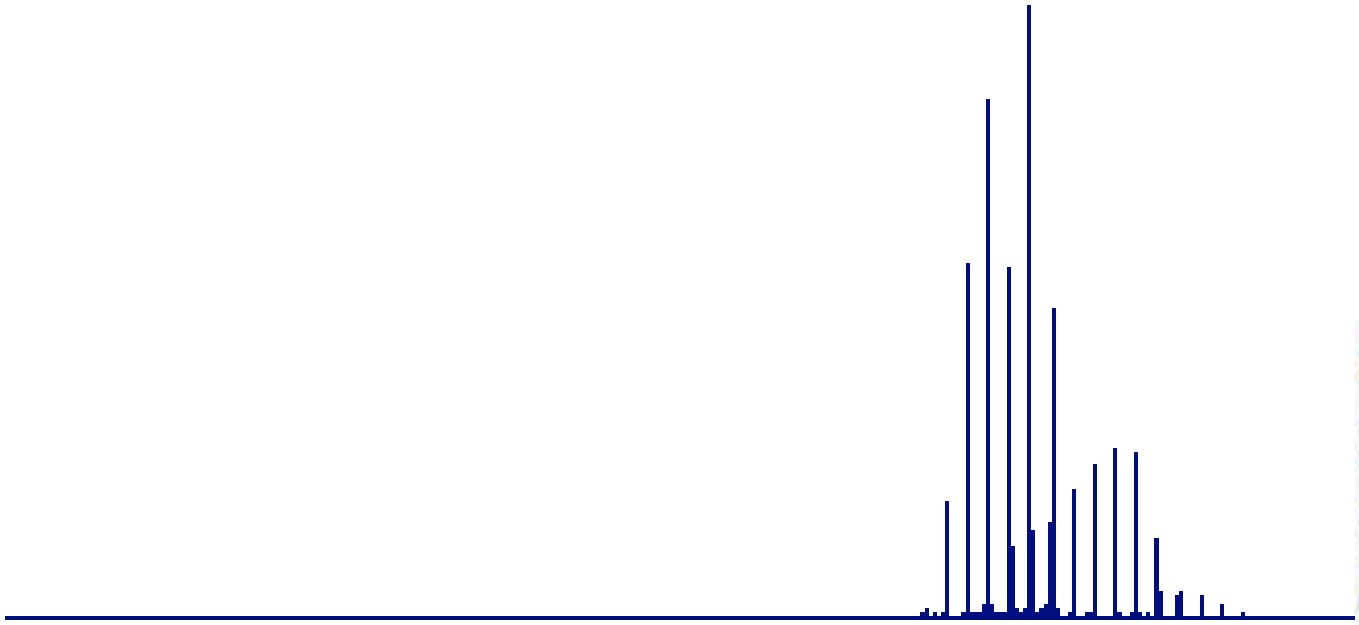
A VERY STRONG property(!).

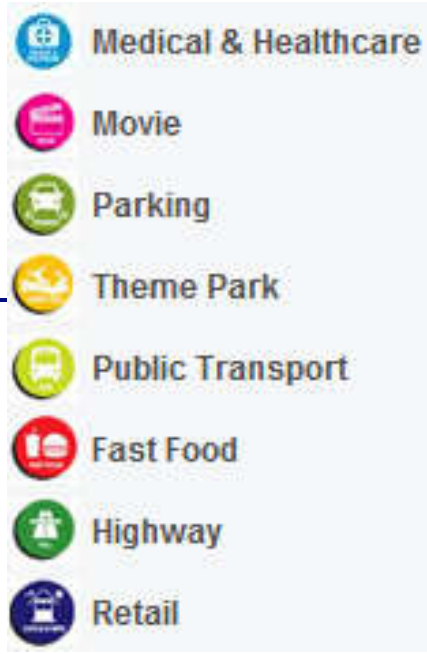
Backdoor 4 – Bad RNG - London University Card



- Looks kind of random
- =>Attack takes very roughly $2^{12.4}$ x 10 s = 1 day/key.

Experiment 2 – Malaysia Payment Card

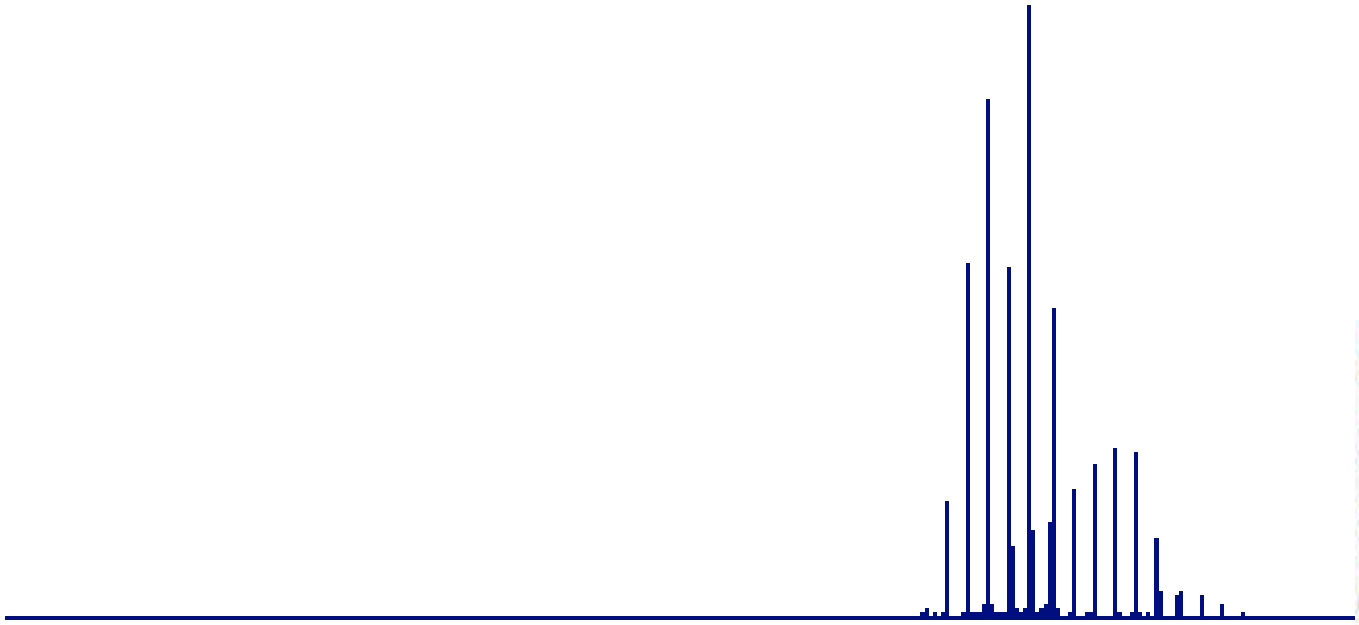


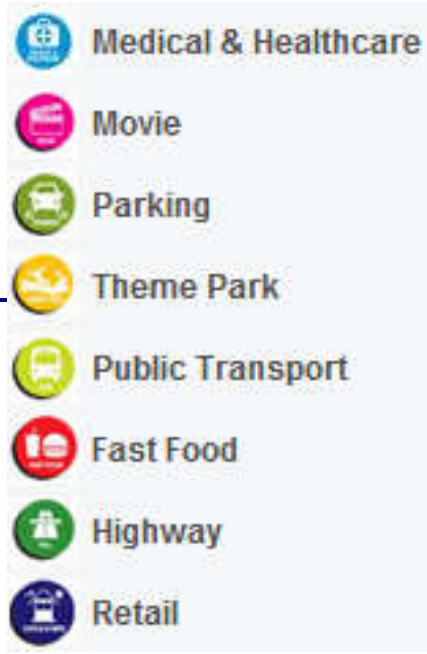


- Attack time $2^{4.4}$ x 10 s = 10 minutes

Courtois

Malaysia – Good News

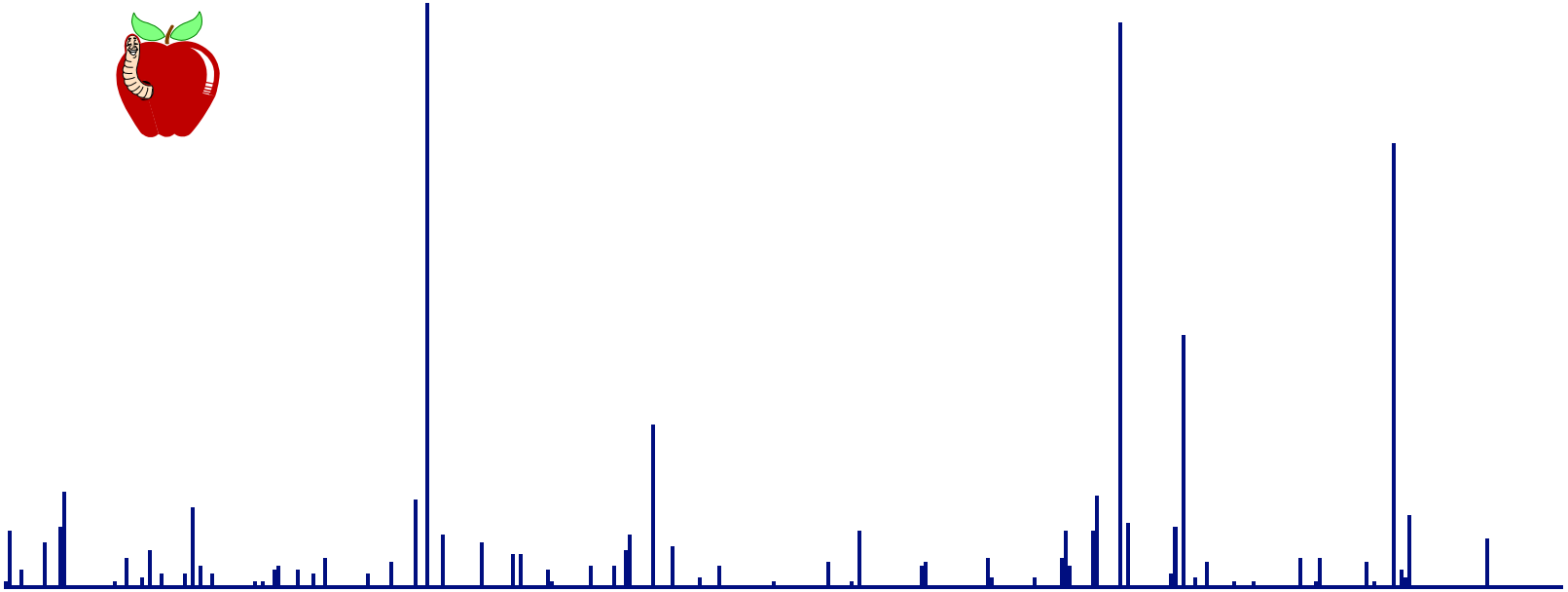




- Each card has different keys ☺
- Not the case for our building card ☹

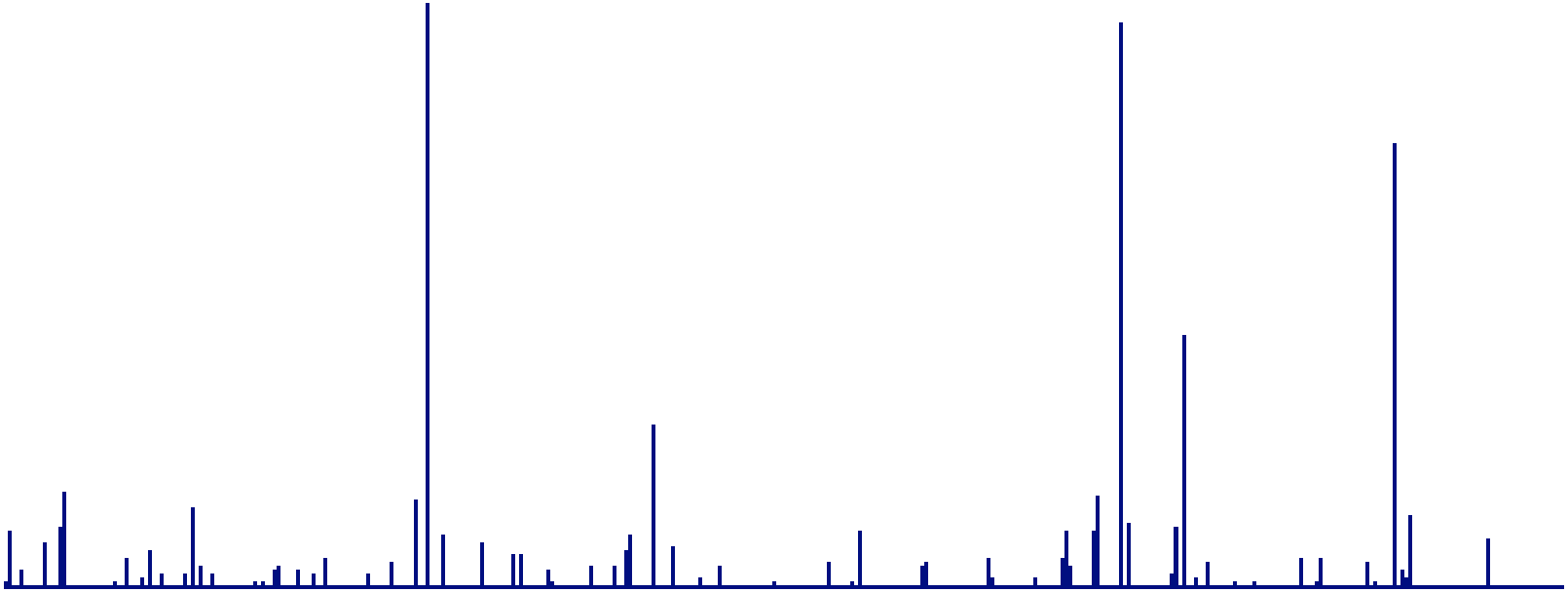
Courtois

London Oyster Card From 2006



- Min-entropy = 2.8 bits.
- Attack time $2^{2.8}$ x 10 s = 3 minutes
-

London Oyster Card – Good News



- Each card has different keys ☺, online fraud detection, 2007 cards already more secure, but this one still in use ☹

Courtois

“Courtois Dark Side” Attack on MiFare Classic

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

It is a multiple differential attack.

Form of multiple “self-similarity” as well..

I exhibit a differential that

- holds simultaneously for 256 differentials this works with probability of about 1/17.
- for 8 differentials the probability is about 0.75 (!!).

Both are differences on 51 bits of the state of the cipher.

A VERY STRONG property(!).

Summary

- We broke 2 billion smart cards covering 70 % of the contactless card/badge/ticketing market.

- Our attack is more than 10 times better than the Dutch attacks about which there were 10 000 press reports
- Data Complexity: 300 queries on average.
- No precomputation. $T = C*2^{21}$.
- More than 10x better than any other attack…
  - in comparison 3rd Nijmegen Oakland attack requires:
  - pre-computed 384 Gbytes of data (EXPENSIVE)
  - 4000 queries… (done in 2 minutes).

Hall of Shame

- In Warsaw, Poland, the first block uses the default Philips key FFFFFFFFFFFF,
- Then keys are THE SAME in every card

Courtois

Hall of Shame (contd.)

- In Warsaw, Poland, the first block uses the default Philips key FFFFFFFFFFFF,
- Then keys are THE SAME in every card
- Moreover keys are NOT random, but human-generated.
  - for example many start with 898989, some end with 898989…
    - obsession with history?
      - in 1989 Poland had first “free” elections…

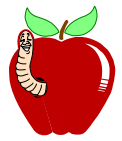
Courtois

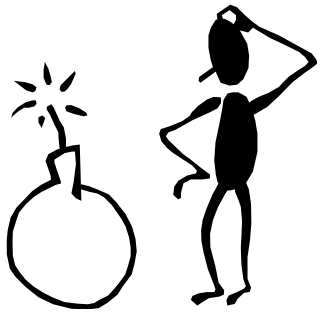
Open Problems

– Backdoor symmetric encryption?

Question:

Why 0% of symmetric encryption used in practice are provably secure?





MQ Problem

Dense MQ is VERY hard. Best attacks ≈ $2^{0.8765n}$

- Top of the top hard problem. mqchallenge.org FXL/Joux 2017/372
- For both standard and PQ crypto.

=> Allows to build a provably secure stream cipher based on MQ directly!

C. Berbain, H. Gilbert, and J. Patarin:

QUAD: A Practical Stream Cipher with Provable Security, Eurocrypt 2005

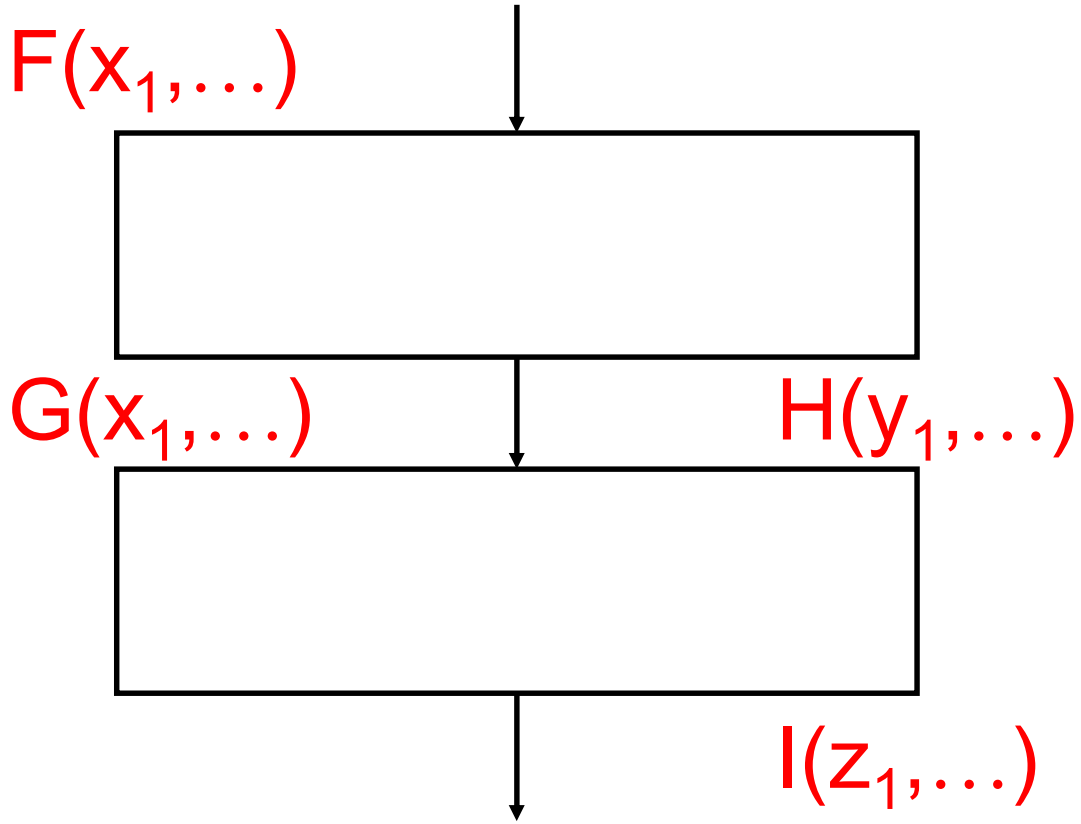
- open problem: design a provably secure block cipher…

Generalised Linear Cryptanalysis = GLC =

[Harpes, Kramer and Massey, Eurocrypt'95]

Connecting Non-linear Approxs.

Non-linear functions.



Generalised Linear Cryptanalysis = GLC =

[Harpes, Kramer and Massey, Eurocrypt'95]

Concept of non-linear I/O sums.

F(inputs) = F'(outputs)

with some probability…

GLC and Feistel Ciphers ?

[Knudsen and Robshaw, EuroCrypt'96]

For some reason decided that…GLC was impossible for Feistel Ciphers. Write that:

"one-round approximations that are non-linear […] cannot be joined together"…

GLC and Feistel Ciphers ?

[Knudsen and Robshaw, EuroCrypt'96

"one-round approximations that are non-linear […] cannot be joined together"…

At Crypto 2004 Courtois shows that GLC is in fact possible for Feistel schemes!

BLC better than LC for DES

$$(*)\quad \begin{aligned} &L_0[3,8,14,25] \oplus L_0[3]R_0[16,17,20] \oplus R_0[17] \oplus \\ &L_{11}[3,8,14,25] \oplus L_{11}[3]R_{11}[16,17,20] \oplus R_{11}[17] = \\ &K[sth] + K[sth']L_0[3] + K[sth'']L_{11}[3] \end{aligned}$$

Better than the best existing linear attack of Matsui

for 3, 7, 11, 15, … rounds.

Ex: LC 11 rounds: $\frac{1}{2} \pm 1.91 \cdot 2^{-16}$

BLC 11 rounds: $\frac{1}{2} \pm 1.2 \cdot 2^{-15}$

Backdoor Ciphers

Courtois AES'2004:

- constructions of pathologically weak ciphers with EXTREMELY high-nonlinearity
- way stronger than DES, AES and any other industrial cipher if you look at the Boolean functions used

Bi-linear Cryptanalysis – Example:

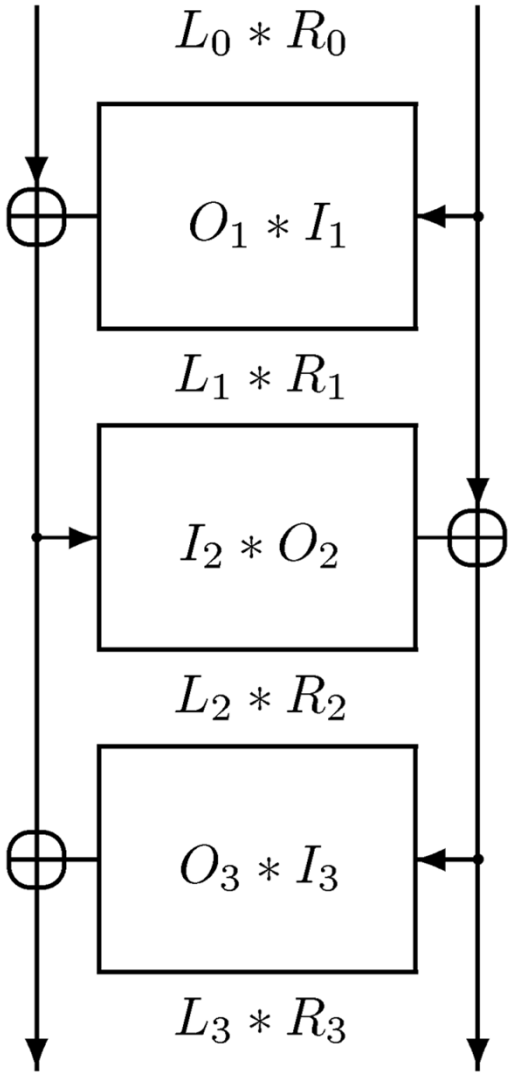
Round function:

$$f_i(X) = K_i \cdot Inv(X) \qquad \text{in } GF(2^n),$$

Then for every round:

$$I_i \cdot O_i = K_i \quad \text{with probability} \quad \left(1 - \frac{1}{2^n}\right)$$

Sum-Up:



$$= L_1 * R_1 - L_0 * R_0$$

$$= L_2 * R_2 - L_1 * R_1$$

$$= L_3 * R_3 - L_2 * R_2$$

Example - contd.

Whole cipher:

$$L_{N_r} \cdot R_{N_r} \oplus L_0 \cdot R_0 = \sum_{i=1}^{N_r} K_i$$

with probability $\left(1 - \frac{1}{2^n}\right)^{N_r}$

Broken even for 2^n rounds !

Another Weak Cipher

Round function:

$$f_i(X) = Inv(X) \cdot (K_i \oplus G(X))$$

$$\text{in } GF(2^n)$$

G – arbitrary component with S-boxes, MDS mixing … [with a small imperfection, see my extended slides from Crypto 2004]

Other Constructions…

Another Example of Insecure Cipher

64-bit Feistel cipher, 32-bit round function:

$$\begin{cases} y = \dfrac{x+x'+K_i}{x+c} & \text{in } GF(2^{16}) \\ y' = \dfrac{x+x'+K'_i}{x'+c'} & \text{in } GF(2^{16}) \end{cases}$$

Looks very secure…Etc.

Broken for up to 2^{16} rounds !

Unbalanced Compressing Feistel (e.g. SHA)

This one again looks very secure:

$$\begin{cases} b \leftarrow a \\ c \leftarrow b \\ d \leftarrow c \\ a \leftarrow d + K_i \cdot Inv(a+b+c) \end{cases}$$

Again, broken for up to 2^{16} rounds !

The Attack:

Look at the expression:

$$ab + ac + ad + bc + bd + cd$$

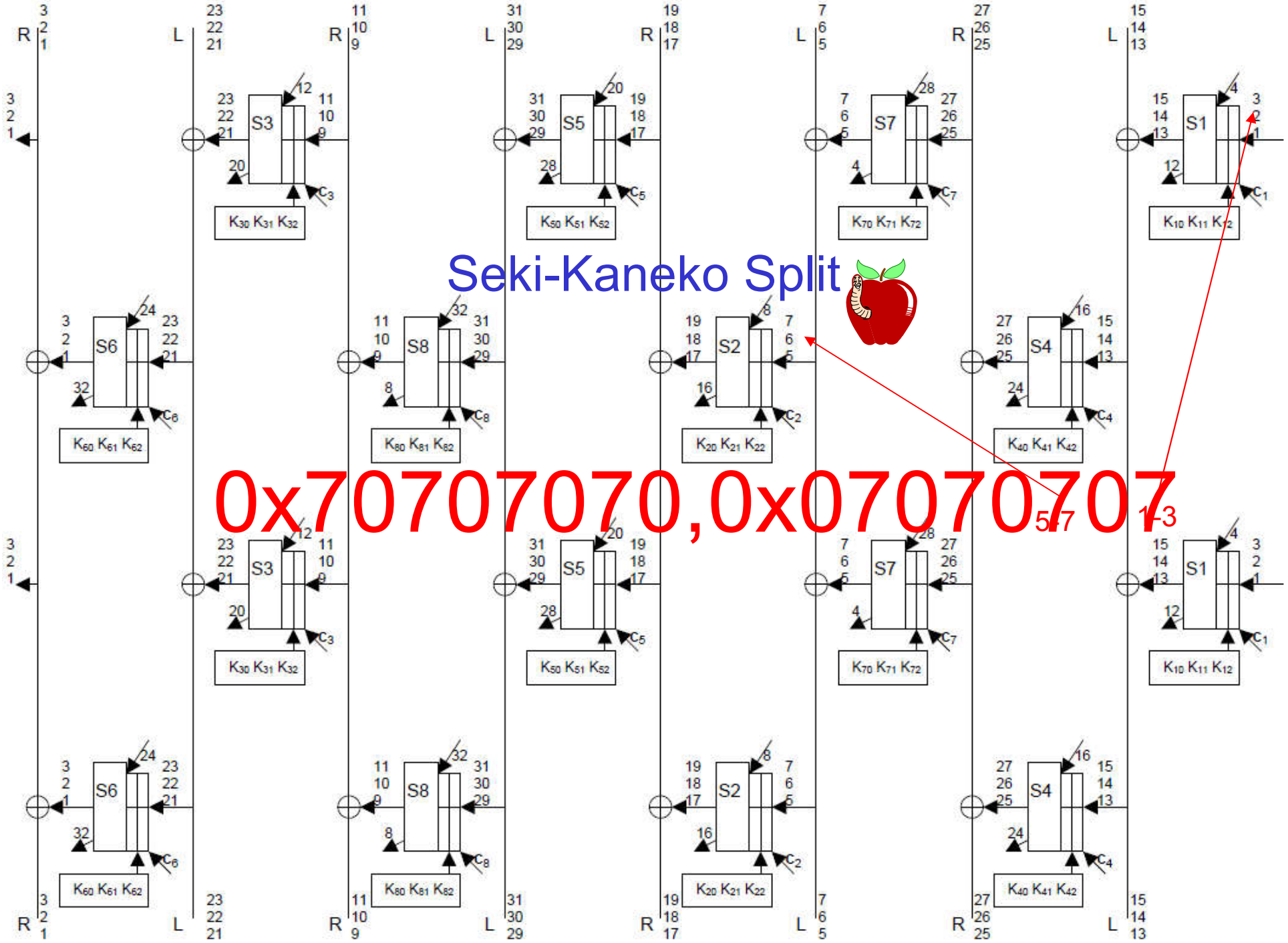
Difference of these for 1 round:

$$ab + ac + ad + bc + bd + cd +$$
$$ab + ac + bc + [d + K_i \cdot Inv(a + b + c)](a + b + c)$$
$$= K_i \cdot Inv(a + b + c) \cdot (a + b + c)$$
$$= K_i \quad \text{with good probability...}$$

5. GOST Cipher

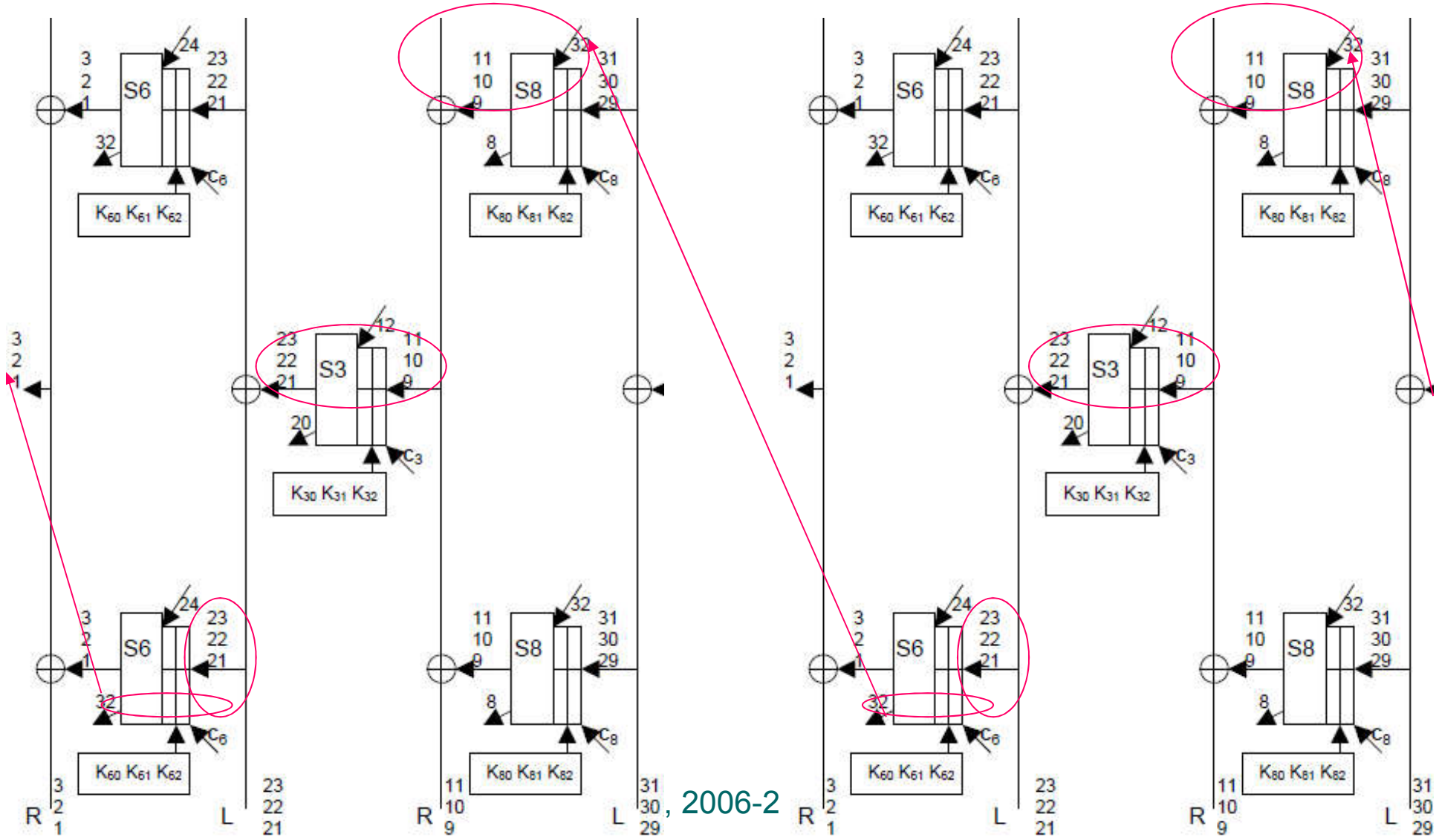
GOST 28148-89

- Developed in the 1970s, or the 1980s,
  - First "Top Secret" / Type 1/Type A algorithm.
  - Downgraded to "Secret" in 1990.
- Declassified in 1994.


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

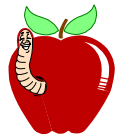
0x80700700,0x80700700 [Courtois-Misztal 2011]

Type 3+3: S836 + S836

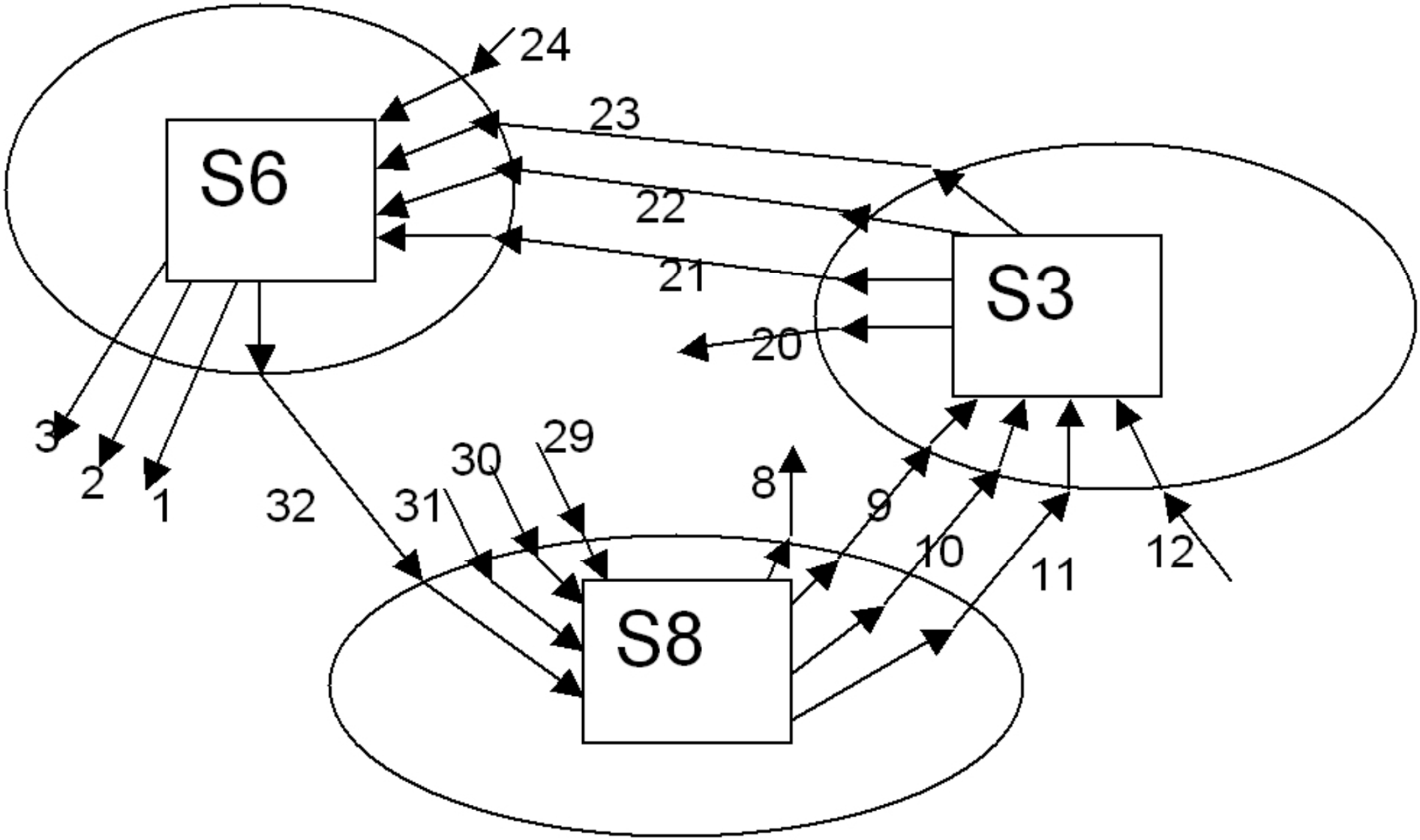


, 2006-2

0x80700700,0x80700700



Type 3+3: S836 + S836



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: $E_k = g_k \circ f_k^8$.

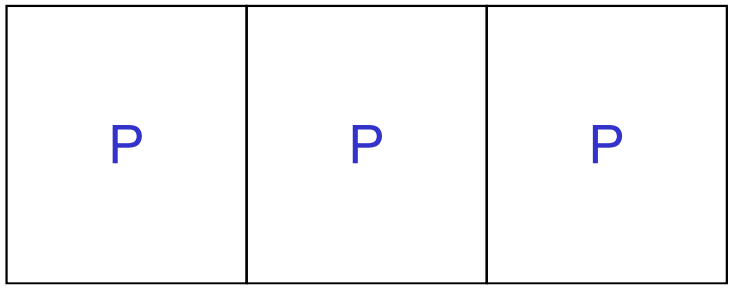
$528 = 16+8*64$ rounds.

4.4. Sliding Properties of KeeLoq

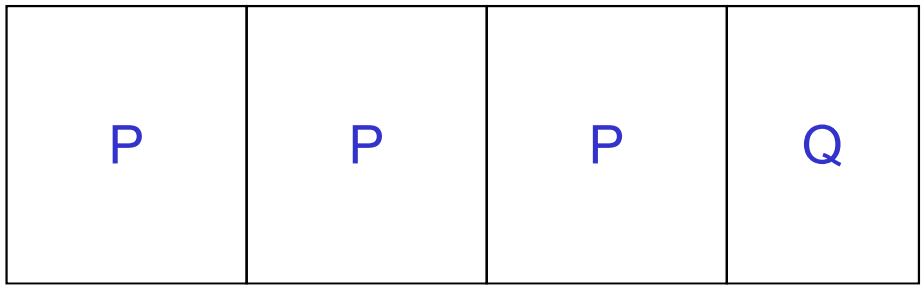
[and one simple attack from FSE 2008]

Sliding Attacks – 2 Cases

- **Complete periodicity [classical].**



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

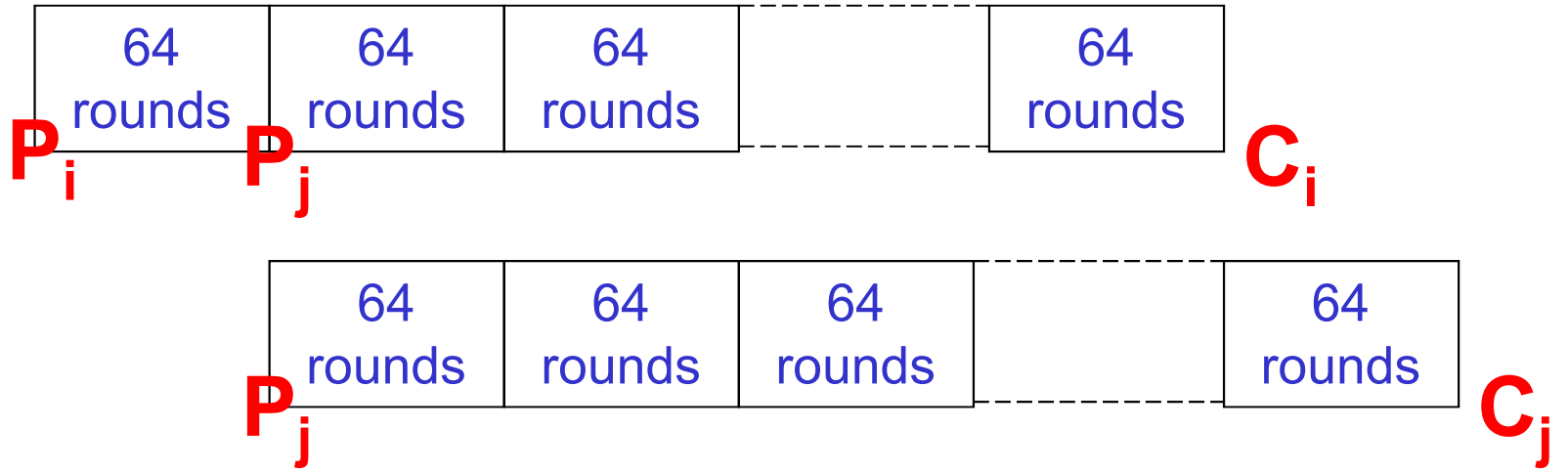


  - **KeeLoq: Q is a functional prefix of P. Helps a lot.**

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.

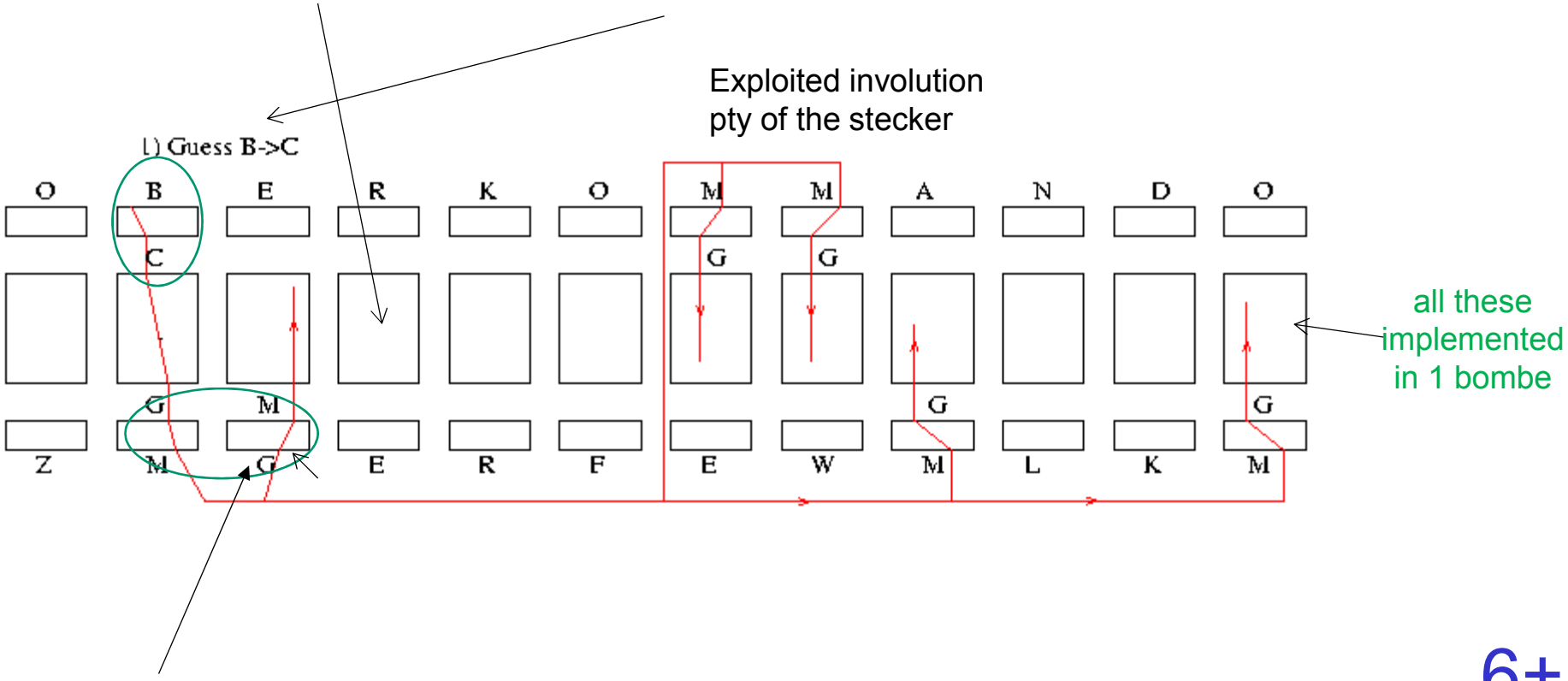


Gives an unlimited number of other sliding pairs !!!

very large **"Amplification"**

WW2 Welchman Bombe Attack a.k.a. Diagonal Board Attack

Testing positions of 3 rotors + 1 P/C pair for S guessed



6+1

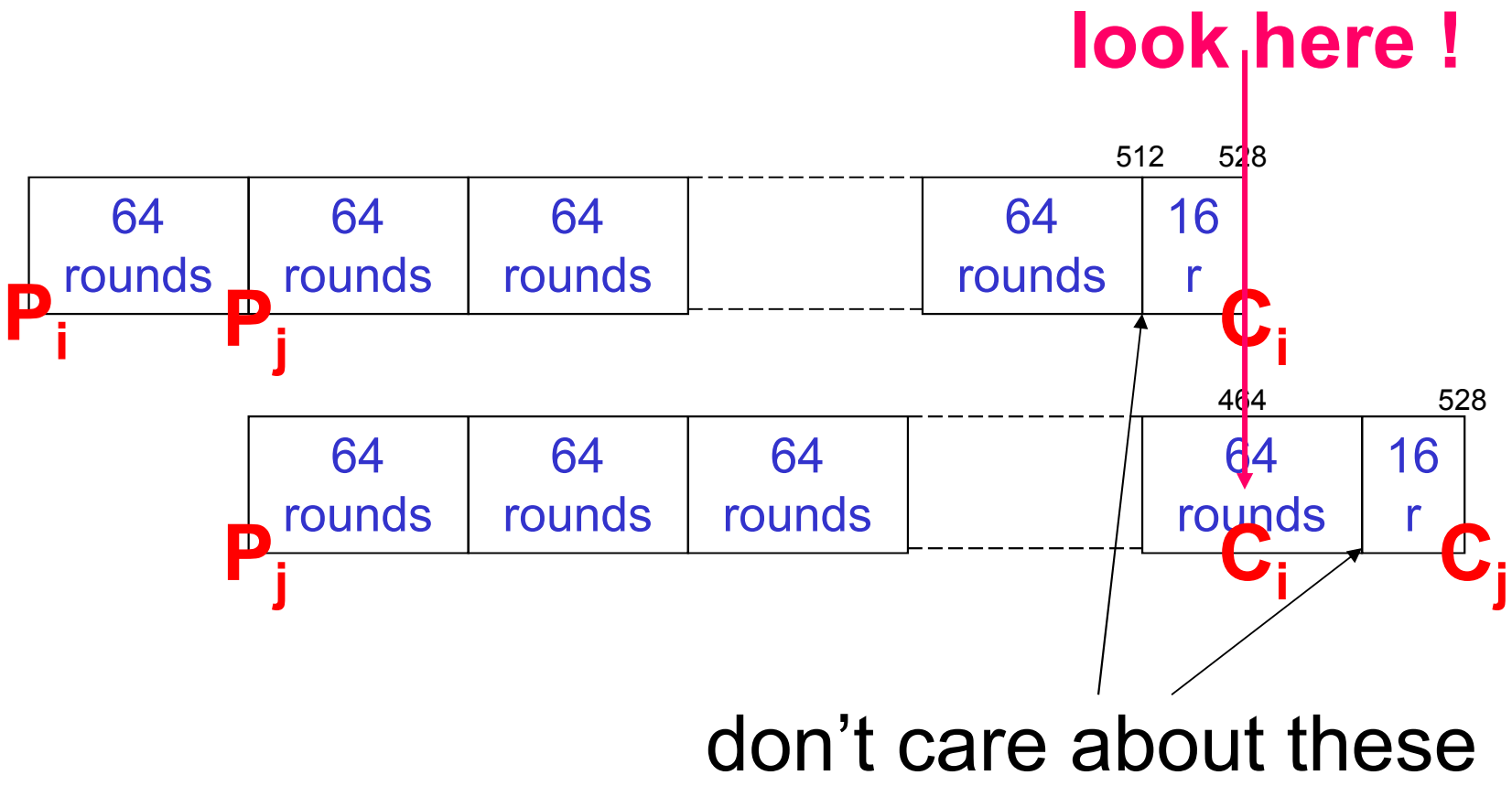
Large amplification, leads to contradiction frequently

KeeLoq [Courtois Bard Wagner FSE 2008]

- 2x Amplification…

Algebraic Sliding

Answer [Courtois, Bard, Wagner FSE2008]:



Algebraic Attack

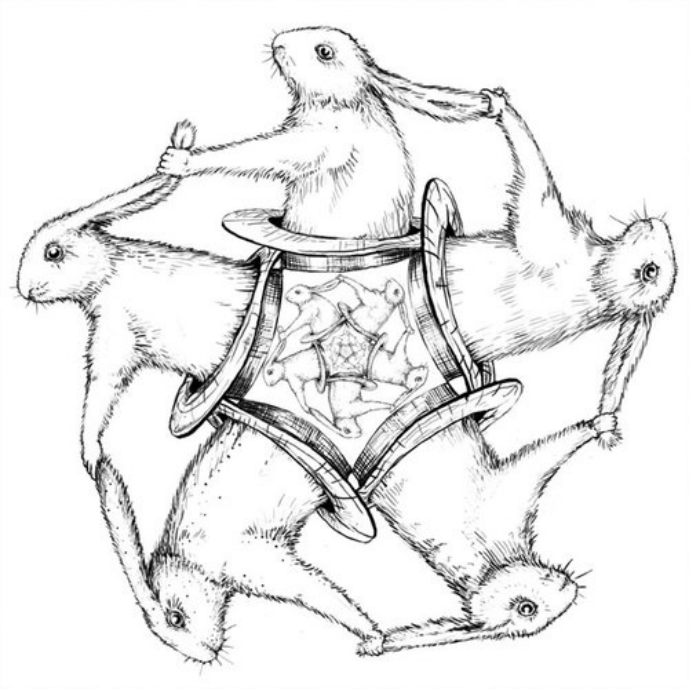
[Courtois Bard Wagner FSE 2008]

We are able to use C_i, C_j directly !

Write and merge 2 systems of equations:

Example to Meditate

Amplification Paradox



Involution => Amplification

1 pair 16 R =>

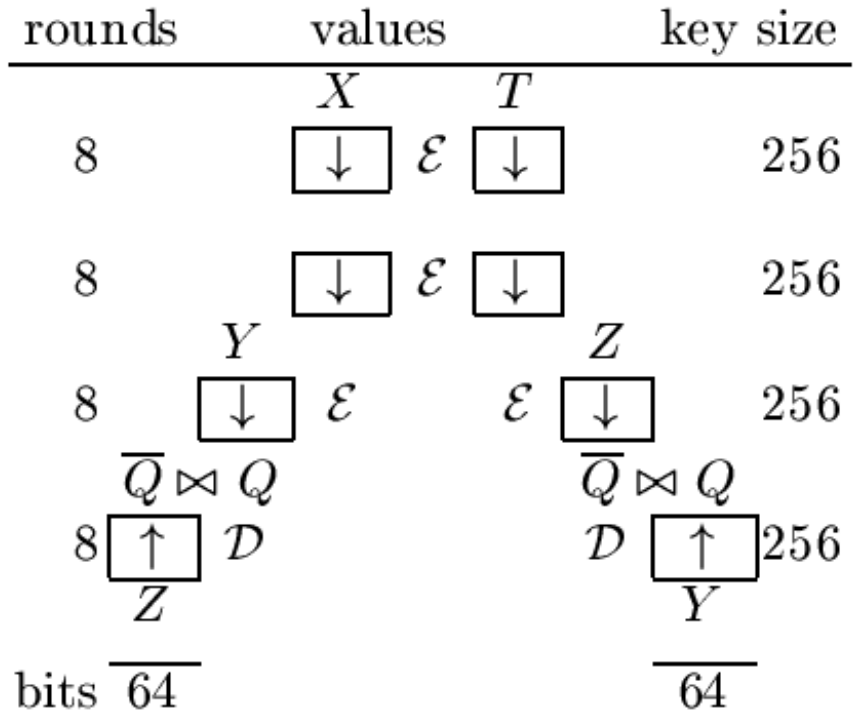
another pair for free

$$Y = \mathcal{E}^2(X)$$

$$\vdash$$

$$Enc_k(X) = \mathcal{E}^2(Dec_k(Y))$$

can we continue?



Bad News

continue?

$$Y = \mathcal{E}^2(X)$$
$$\vdash$$
$$Enc_k(X) = \mathcal{E}^2(Dec_k(Y))$$
$$\vdash$$
$$Enc_k(Dec_k(Y)) = \mathcal{E}^2(Dec_k(Enc_k(X)))$$

Important provable security corollary:

cannot hope to prove security!