Algebraic and Slide Attacks on KeeLoq

Nicolas T. Courtois [1]
Gregory V. Bard [2]
David Wagner [3]

[1] - University College of London, UK

[2] - Fordham University, NY, US

[3] - University of California - Berkeley, US

Roadmap

- KeeLoq.
- Direct algebraic attacks,
  - 160 rounds / 528.

Periodic structure =>

- Slide-Algebraic:
  - 2^{16} KP and about 2^{53} KeeLoq encryptions.
- Slide-Determine:
  - 2^{23} - 2^{30} KeeLoq encryptions.

KeeLoq

Block cipher used to unlock doors and the alarm in Chrysler, Daewoo, Fiat, GM, Honda, Jaguar, Toyota, Volvo, Volkswagen, etc…

Courtois, Bard, Wagner, FSE 2008

Our Goal:

To learn about cryptanalysis…

Real life: brute force attacks with FPGA's.

How Much Worth is 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, <u>main reason:</u>

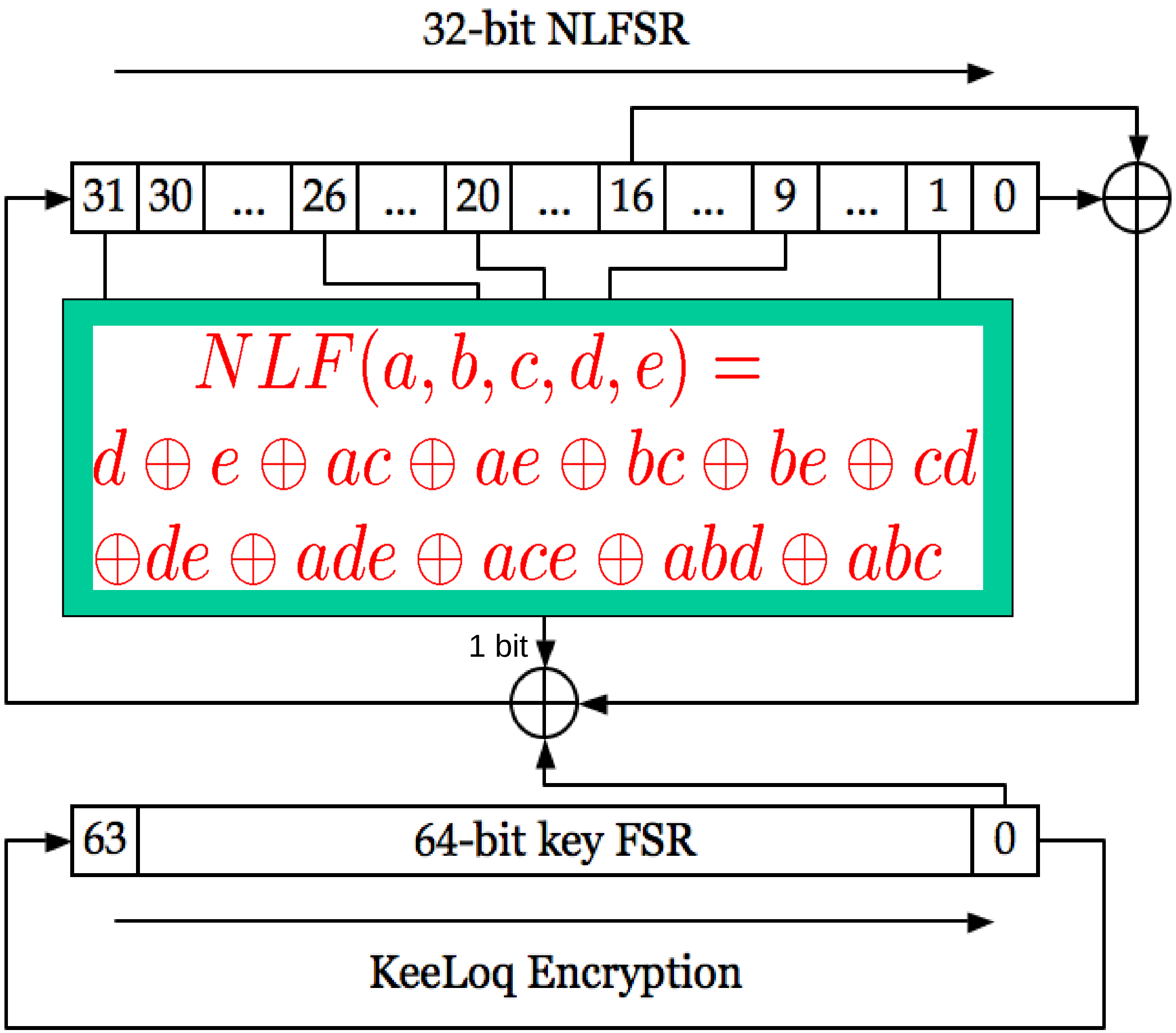
its periodic structure: cannot be defended. The complexity of most attacks on KeeLoq does NOT depend on the number of rounds of KeeLoq.

Courtois, Bard, Wagner, FSE 2008

Remarks

- Paying 10 million $ for a proprietary algorithm doesn’t prevent it from being very weak.
- In comparison, RSA Security has offered (“only”) 70 K$ as a challenge for breaking RC5.
  - For much less money they have the algorithm that (visibly) nobody can break.
- For AES there is no challenge/price, not even 1 dollar, and according to an Internet survey (cf. www.cryptosystem.net/aes/), 40 % of people tend to believe that AES is already broken…

Description of KeeLoq



KeeLoq Encryption

Block Cipher

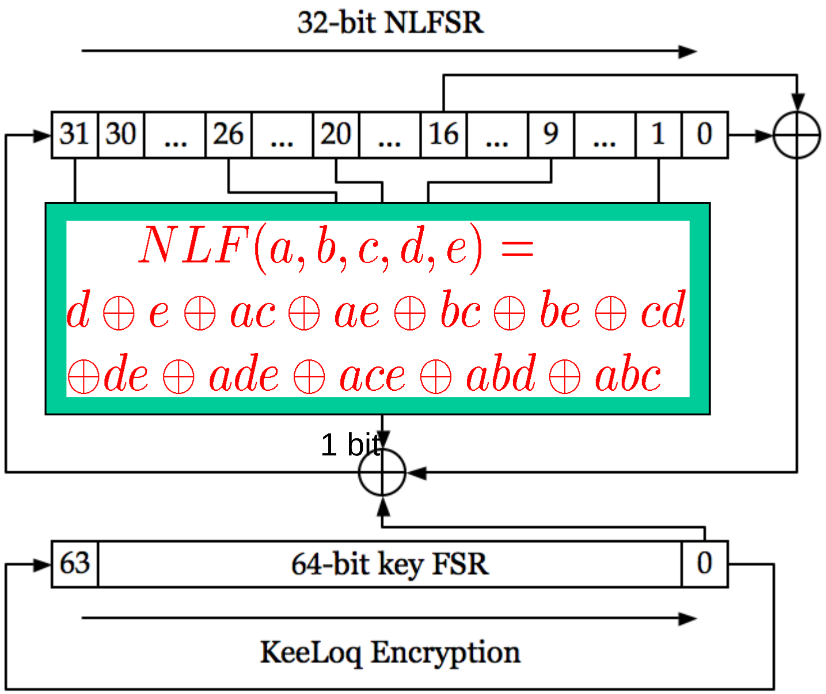
- Highly unbalanced Feistel
- 528 rounds
- 32-bit block / state
- 64-bit key
- 1 bit updated / round
- 1 key bit / round only !

Sliding property:

periodic cipher with period 64.

Courtois, Bard, Wagner, FSE 2008

Complete Description



1. Initialize with the plaintext: $L_{31}, \ldots, L_0 = P_{31}, \ldots, P_0$
2. For $i = 0, \ldots, 528 - 1$ do

   $L_{i+32} = k_{i \ mod \ 64} \oplus L_i \oplus L_{i+16} \oplus NLF(L_{i+31}, L_{i+26}, L_{i+20}, L_{i+9}, L_{i+1})$
3. The ciphertext is $C_{31}, \ldots, C_0 = L_{559}, \ldots, L_{528}$.

Figure 1: KeeLoq Encryption

Courtois, Bard, Wagner, FSE 2008

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.

Attacks on KeeLoq

Algebraic Attacks on KeeLoq

KeeLoq can be implemented using about 700 GE.

=> “direct” algebraic attack: write equations+solve.

Two methods:

- ElimLin/Gröbner bases
- Conversion+SAT solvers.

Algebraic Attacks on KeeLoq

We have found MANY attacks.

This paper: only two of them.

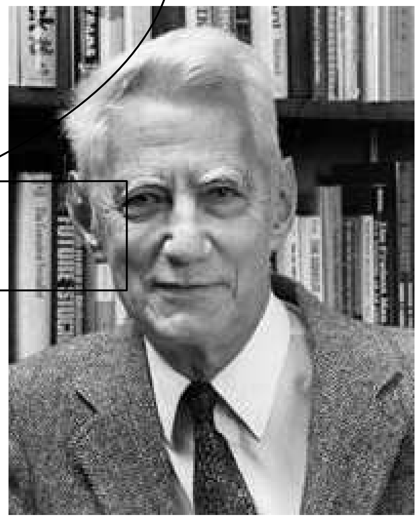
(the fastest ever found – not algebraic
and the simplest ever found - algebraic)

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]



What Can Be Done ?

As of today, we can:

ElimiLin (Method 1):

With ElimLin we can break up to 128 rounds of KeeLoq faster than brute force.
128 KP counter mode.

Conversion+MiniSAT (Method 2):

Also up to 160 rounds of KeeLoq but
2 known plaintext (cannot be less).

Our Equations

Can be downloaded from:

www.cryptosystem.net/aes/toyciphers.html

Beyond?

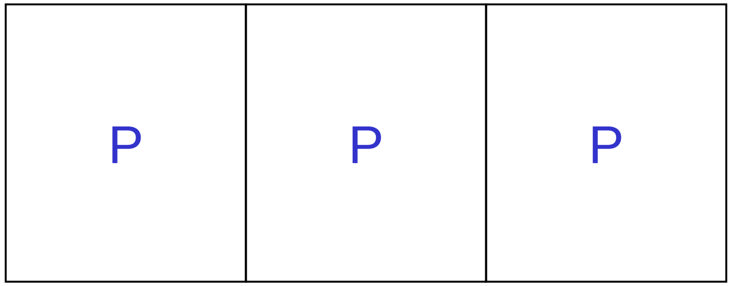
KeeLoq has additional weaknesses.

There are much better attacks.

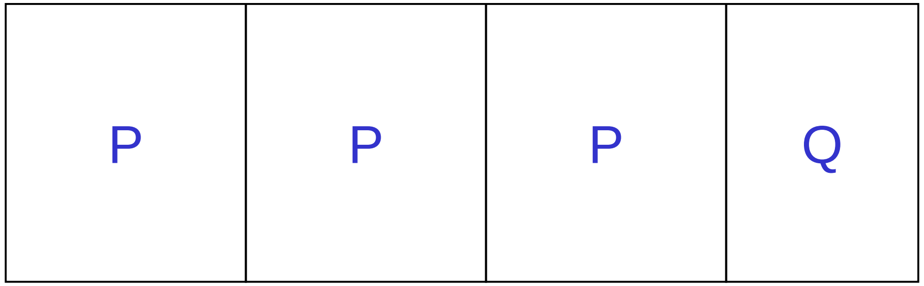
Sliding Attacks

Sliding Attacks – 2 Cases

- **Complete periodicity [classical].**



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

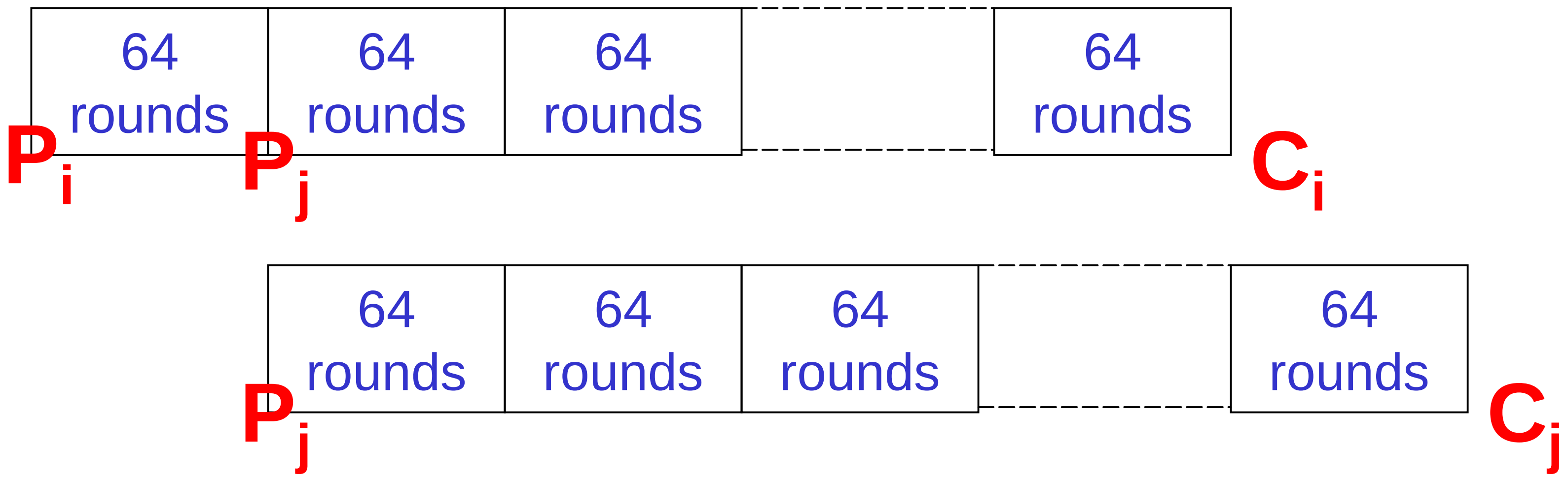


  - **KeeLoq: Q is a functional prefix of P. Helps a lot.**

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.

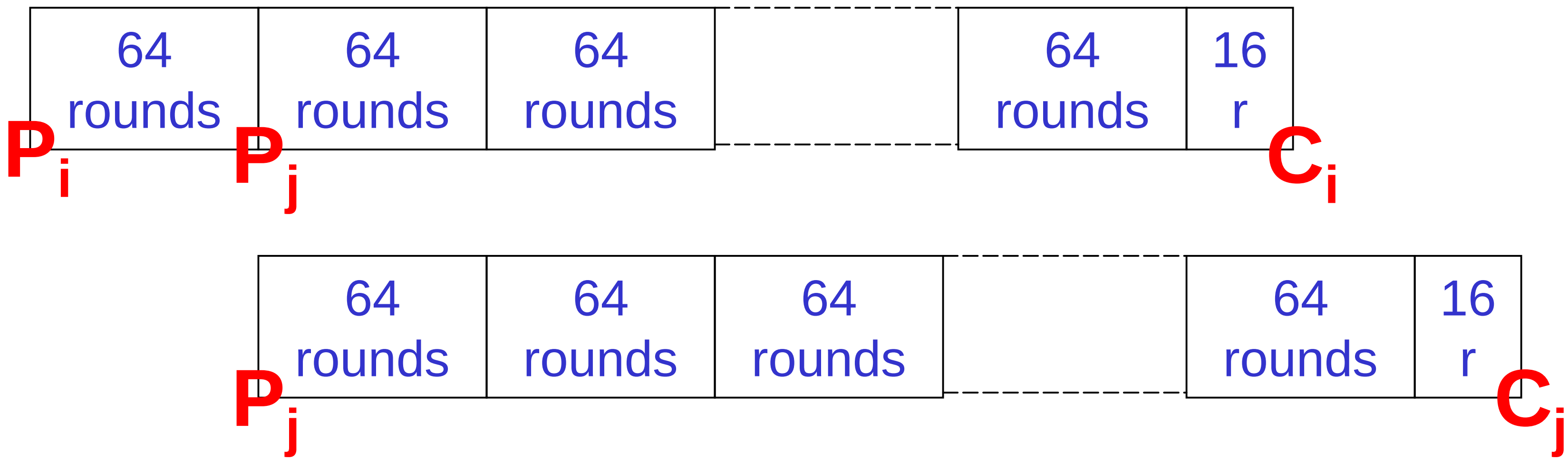


Gives an unlimited number of other sliding pairs !!!

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.

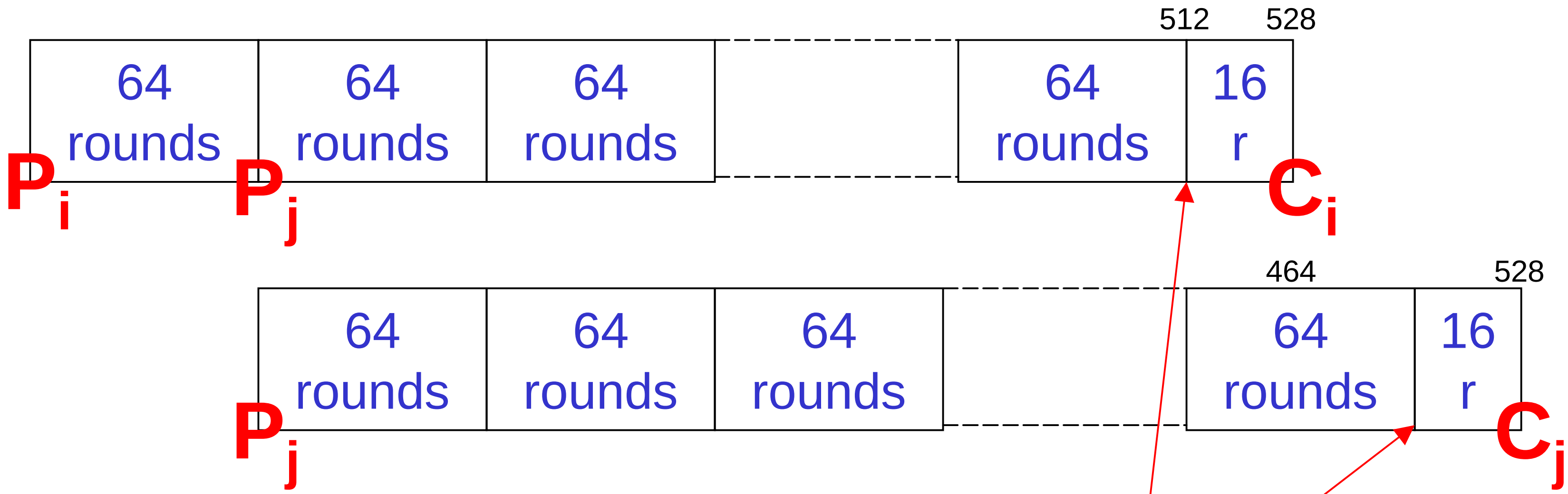


Classical sliding fails – because of the “odd” 16 rounds:

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 ?

Roadmap for KeeLoq

guess 16 key bits

correct?

sliding-algebraic

Attack 2

batch guess fixed points

Slide-Algebraic
Slide-Determine

direct 528 rounds

LC,DC,AC fail…

key recovery attacks on f_k - 64 rounds only
(recover key, confirms the 16 bits)

direct confirmation!
(unknown key)

distinguisher for P^8

eprint, not published

*Attack 1 [Attack 5] LC ….

Courtois, Bard, Wagner, FSE 2008

Roadmap for KeeLoq

guess 16 key bits

sliding-algebraic

Attack 2

batch guess fixed points

Slide-Algebraic

Slide-Determine

direct 528 rounds

LC,DC,AC fail…

three new types of sliding attacks

….

Guess and Confirm Attacks

guess 16 key bits

correct?

key recovery attacks on f_k - 64 rounds only
(recover key, confirms the 16 bits)

direct confirmation!
(unknown key)

Attack 3

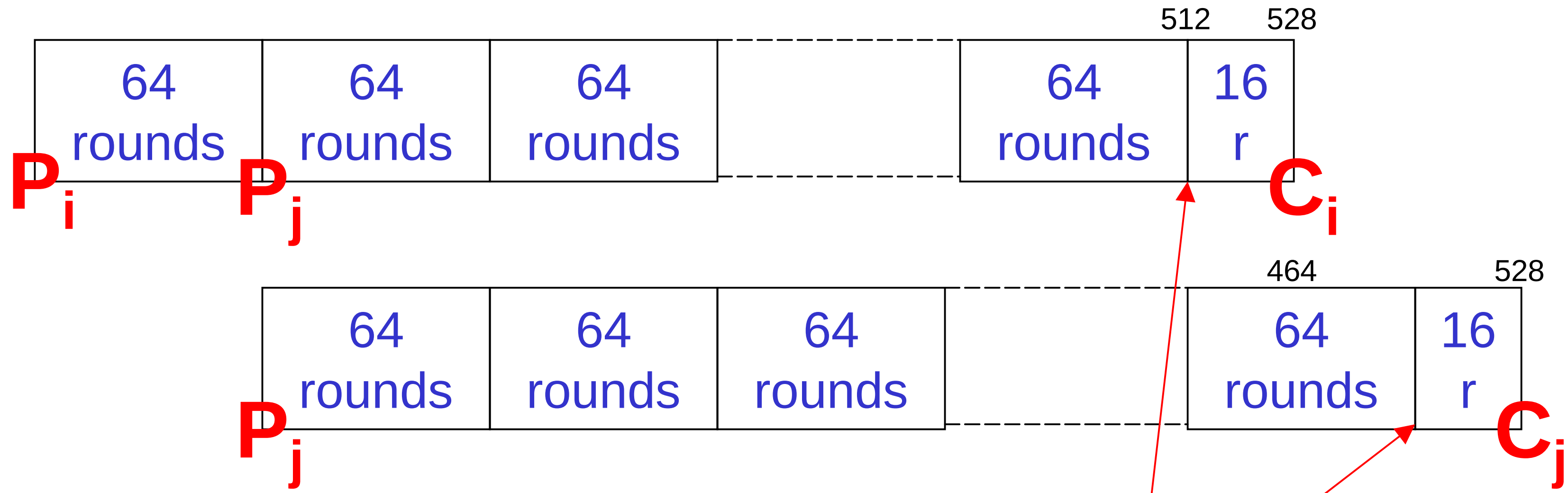
*Attack 1 [Attack 5] LC ….

Courtois, Bard, Wagner, FSE 2008

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).

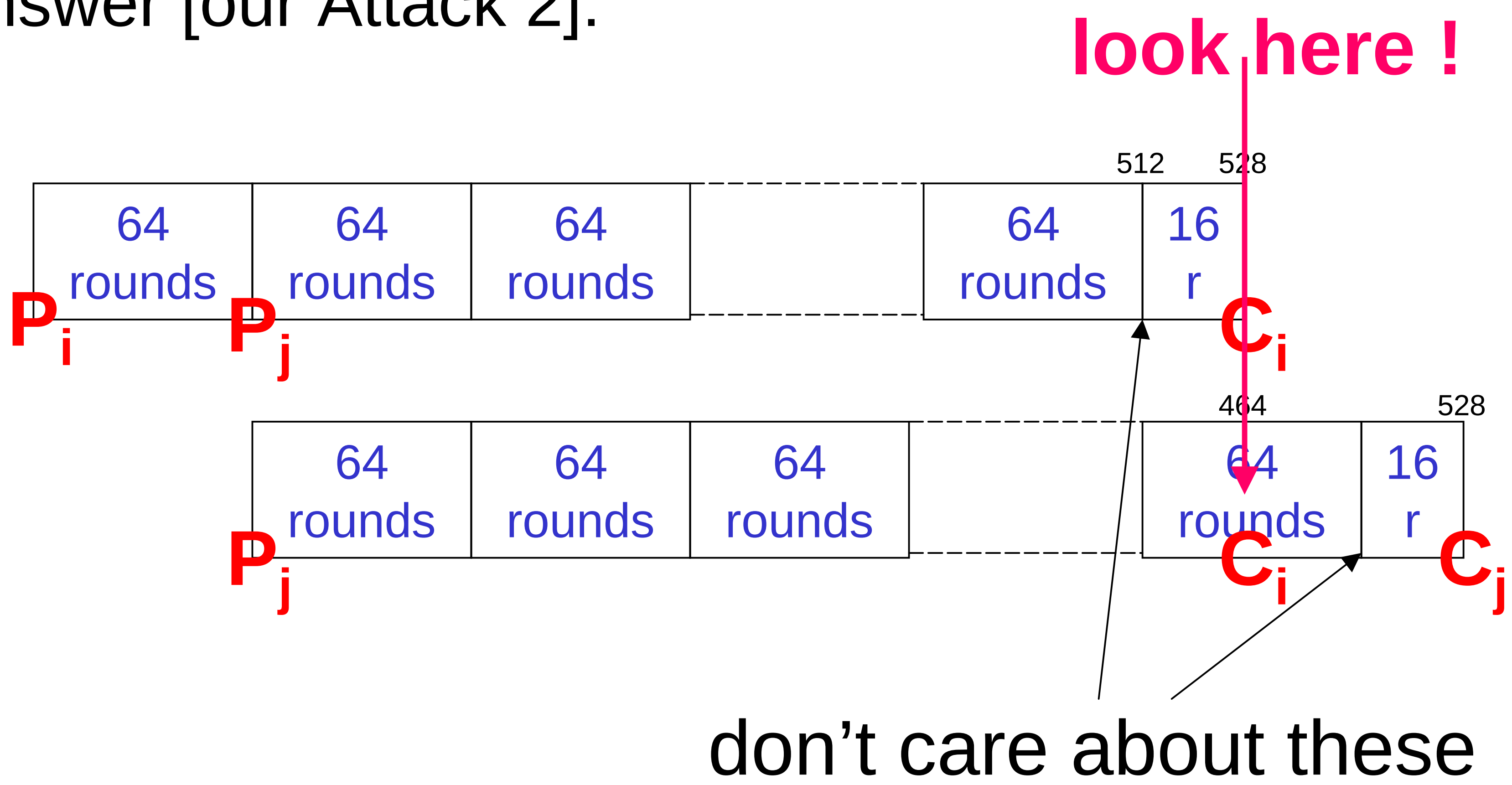


HARD - Problem:

What's the values here ?

Algebraic Sliding

Answer [our Attack 2]:



Algebraic Attack:

We are able to use C_i,C_j directly !

Merge 2 systems of equations:

Courtois, Bard, Wagner, FSE 2008

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.

KeeLoq is badly broken.

Practical attack, tested and implemented.

Conclusion

For the first time ever,
a full industrial block cipher have been totally broken by an algebraic attack.

The full key can be recovered on a PC given 2^{16} KP.

What Happened?

Power of Algebraic Attacks: Any cipher that is not too complex is broken… (!)

– Problem: We hit the “wall” when the number of rounds is large.

Power of Sliding Attacks: their complexity does NOT depend on the number of rounds.

These two combined give a first in history successful algebraic attack on an industrial block cipher.

Faster Attacks on KeeLoq

Algebraic Attacks on KeeLoq

Much faster attacks are possible (!)

With about 2^{32} KP.

The whole dictionary

(in fact a proportion, like 60% can be sufficient)

(Our fastest Slide-Determine Attack
is equivalent to 2^{23} KeeLoq encryptions.
As fast as reading the dictionary.

Mush faster than obtaining 2^{32} KP.

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.

Random Functions

n bits -> n bits

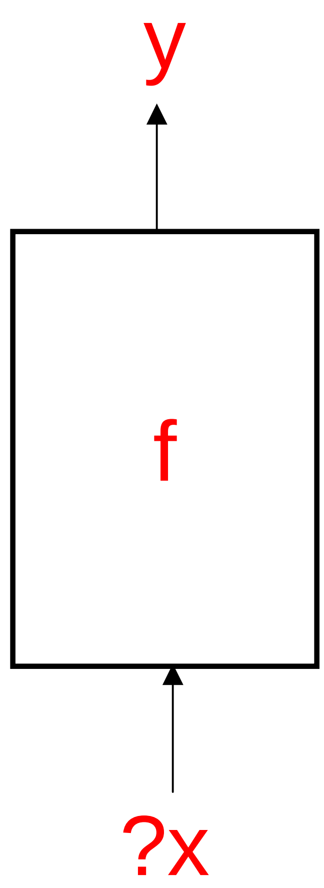
The probability that a given point has i pre-images is 1 / ei!.

<u>Fixed points:</u>

number of fixed points of f(x) ⇔

number of points such that g(x)=0

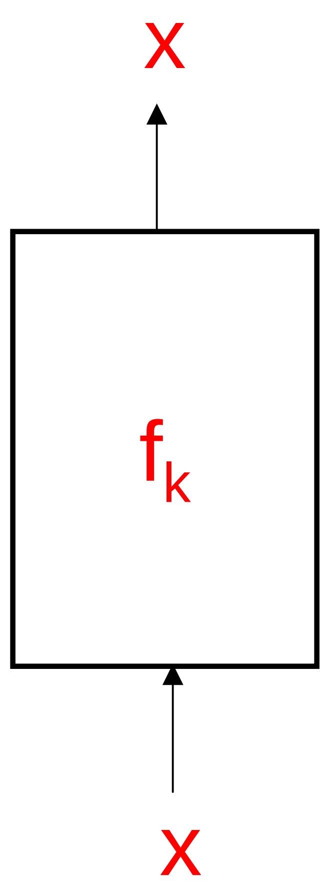
with g(x) = f(x)-x .



Fixed Points for 64 rounds of KeeLoq

f_k is expected to have 1 fixed points for 1-1/e ≈ 0.63 of all keys.

f_k is expected to have 2 fixed points for 1-2/e ≈ 0.26 of all keys.

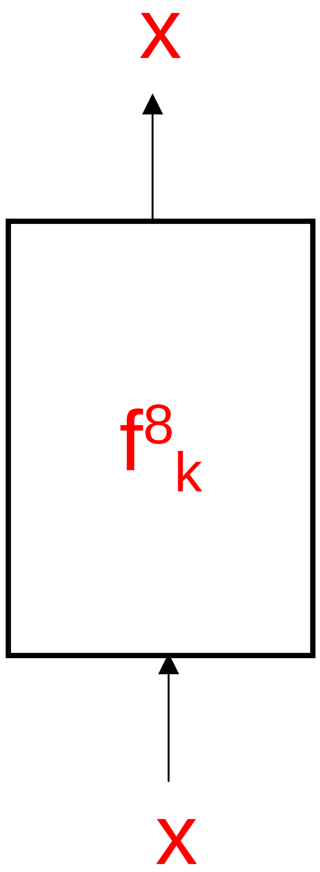


Fixed Points for 512 rounds

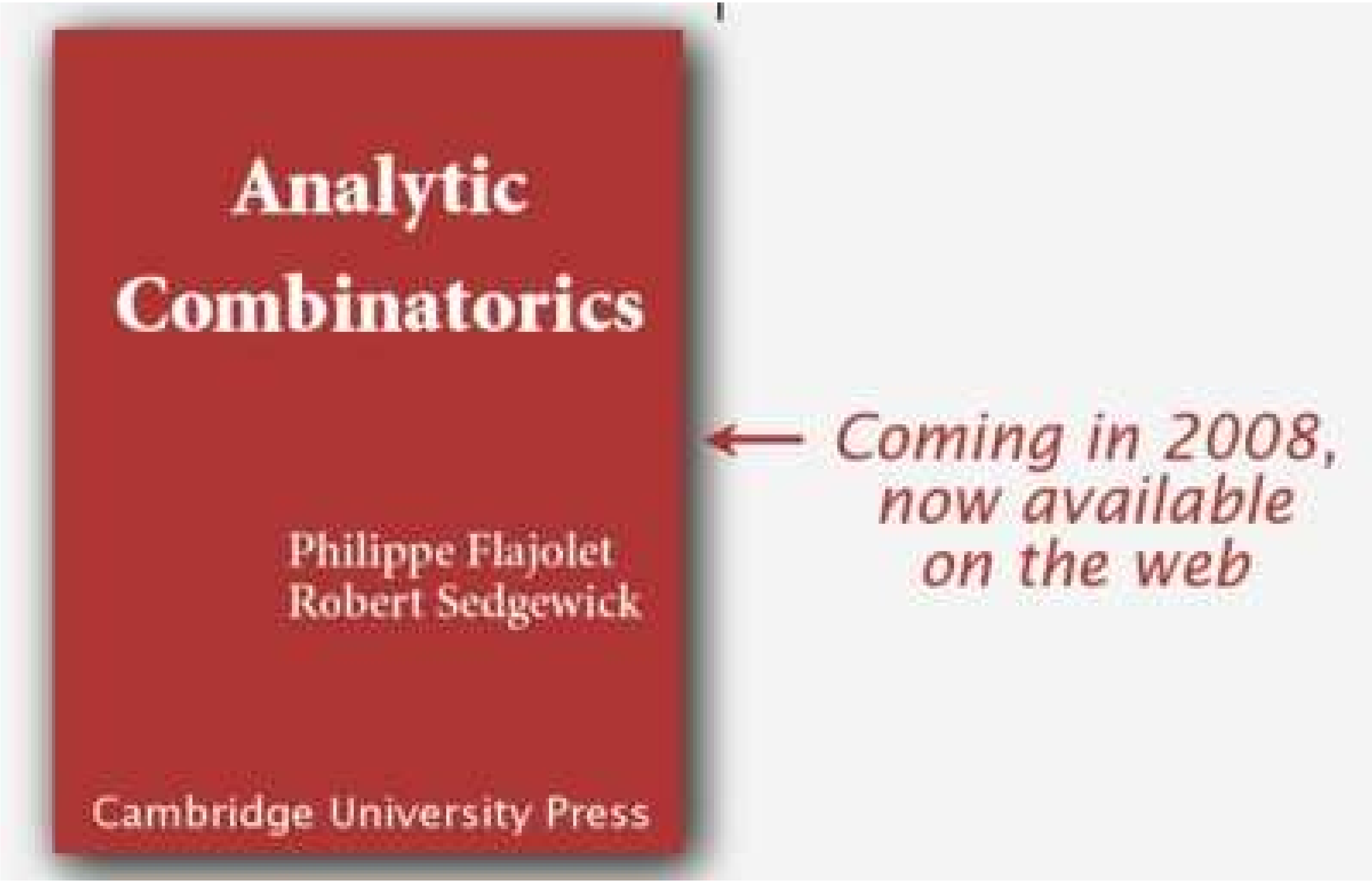
Theorem.

f^8_k has exactly 4 fixed points on average.

We can prove it for random permutations.



How to Solve It?



Theorem [Flajolet, Sedgewick page 132]

Proposition C.2. Let $\mathcal{A} \subset \mathbb{N}_+$ be an arbitrary subset of cycle lengths, and let $\mathcal{B} \subset \mathbb{N}_+$ be an arbitrary subset of cycle sizes. The class $\mathcal{P}^{(\mathcal{A},\mathcal{B})}$ of permutations with cycle lengths in A and with cycle number that belongs to B has EGF as follows:

$$g(z) = \mathcal{P}^{(\mathcal{A},\mathcal{B})}(z) = \beta(\alpha(z)), \qquad \text{where} \;\; \alpha(x) = \sum_{i \in A} \frac{x^i}{i} \;\; \text{and} \;\; \beta(x) = \sum_{i \in B} \frac{x^i}{i!}$$

Theorem [extended version of this paper]

Proposition C.8. Let π be a random permutation and $j, k \in \mathbb{N}_+$. The probability that π^k has exactly j fixed points is:

$$e^{-\sum_{i|k} \frac{1}{i}} \cdot S(j) \quad \text{when} \;\; N \to \infty \quad \text{where} \;\; S(j) = [t^j]\, exp\left(\sum_{i|k} \frac{t^i}{i}\right)$$

More Results [extended version of this paper]

Proposition C.10. Let π be a random permutation and $j, k \in \mathbb{N}_+$. The probability that π^k has exactly j fixed points and π has at least 1 fixed point is:

$$e^{-\sum_{i|k}\frac{1}{i}} \cdot S'(j) \quad \text{when} \quad N \to \infty$$

$$\text{where } S'(j) = [t^j]\, exp\left(\sum_{i|k} \frac{t^i}{i}\right) - [t^j]\, exp\left(\sum_{\substack{i|k \\ i \neq 0}} \frac{t^i}{i}\right)$$

In practice:

j	0	1	2	3	4	5	6	7
$S'(j)$	0	1	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{7}{24}$	$\frac{7}{15}$	$\frac{151}{720}$
$e^{-\sum_{i\|k}\frac{1}{i}} \cdot \sum_{i=j}^{\infty} S'(i)$	0.632	0.632	0.479	0.402	0.300	0.255	0.184	0.151

Courtois, Bard, Wagner, FSE 2008

Our Slide-Determine Attack

Initially started as an Slide-Algebraic Attack 3 in the old paper [eprint].

With time it turned out that the algebraic parts can be totally removed and replaced by faster direct methods…

Our Slide-Determine Attack

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.

Best Batch-Guessing Attack

$E\_k = g\_k \circ f^8\_k$.

Stage 1:

- Assume fixed point for f^8_k - 4 on average!
- Determine 16 key bits [instant]
  – Confirm [NEW makes the attacks much faster!]
- Assume fixed for f_k
  - ⇒ Stage 2. Get a Table of $C*2^{32}$ keys. Easy because 48 ‘small’.
  - ⇒ Stage 3. Confirm which is right. $C*2^{32}$ KeeLoq computations.

Remark:

We have completed the design and analysis of this attack AFTER the pre-proceedings went to print.

We have now very precise analysis with all probabilities and complexities exactly.

Latest Results:

2^{32} KP, 1 fixed point for f_k.

Version 1: Fast RAM (1 CPU clock to read 64 bits, consecutive access, no random access needed).

15 % of keys => 2^{23} KeeLoq encryptions (reading).

Version 2: Realistic RAM (16 CPU clock for 64 bits).

30 % of keys => 2^{27} KeeLoq encryptions (reading).

Version 3: Weighted average.

63 % of keys => $2^{29.6}$ KeeLoq encryptions on average.

2^{32} worst case.

(1-0.63) - Strong Keys of KeeLoq

It is possible, at a manufacturing/personalization stage of KeeLoq, to make sure that f_k has no fixed points !

This excludes 63 % of keys. Effective key size goes down from 64 to 62.6 bits. Small loss !!! Prevents fast attacks.

This solution can be used in practice, and is very similar to a known solution that was in 2002 patented and commercialized by Gemplus (currently Gemalto) to prevent GSM SIM cards from being cloned, see http://www.gemalto.com/press/gemplus/2002/r_d/strong_key_05112002.htm

Results

- Direct algebraic attacks,
  - 160 rounds / 528.

Periodic structure =>

- Slide-Algebraic:
  - 2^{16} KP and about 2^{53} KeeLoq encryptions.
- Slide-Determine:
  - 2^{23} - 2^{30} KeeLoq encryptions.

What Happened?

Power of Algebraic Attacks: Any cipher that is not too complex is broken… (!)

- Problem: We hit the “wall” when the number of rounds is large.

Power of Sliding Attacks: their complexity does NOT depend on the number of rounds.

These two combined give a first in history successful algebraic attack on an industrial block cipher.