Algebraic Techniques in Differential Cryptanalysis

. . . walking that extra mile with algebra

Martin Albrecht and Carlos Cid

Information Security Group,
Royal Holloway, University of London
Egham, Surrey TW20 0EX, United Kingdom

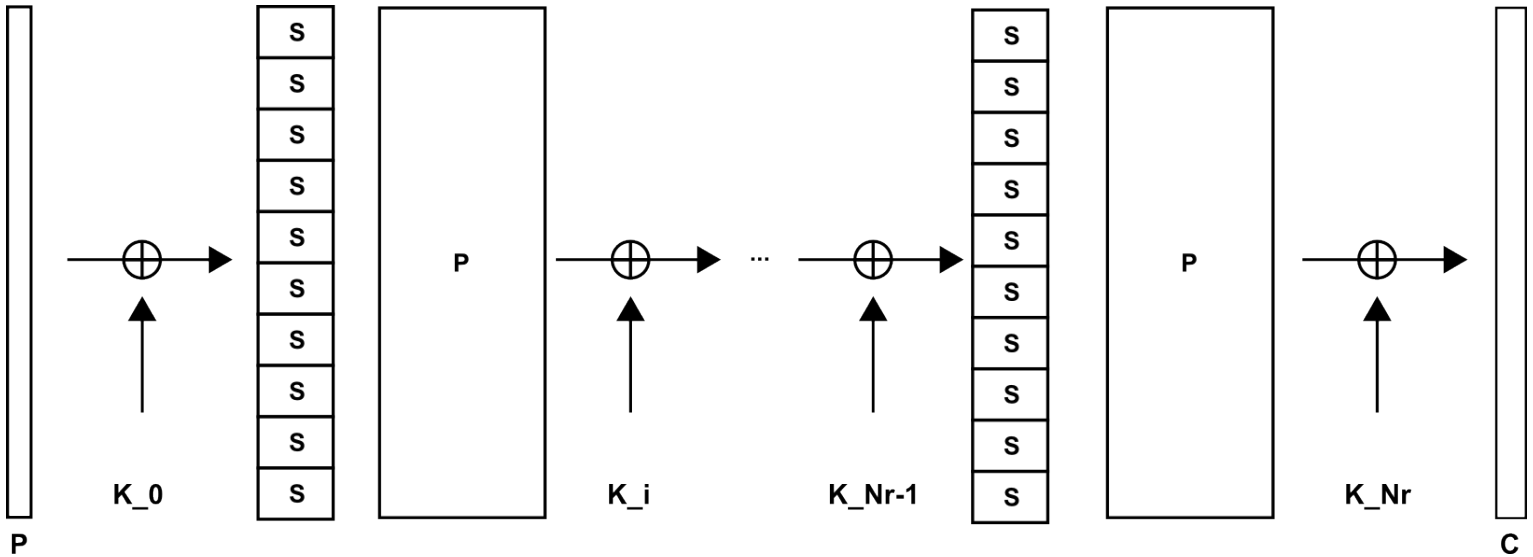
Beijing, 28. April 2008

Outline

Outline

The Blockcipher PRESENT

PRESENT [2] was proposed by Bogdanov et al. at CHES 2007 as an ultra-lightweight block cipher, suitable for RFIDs and similar devices.

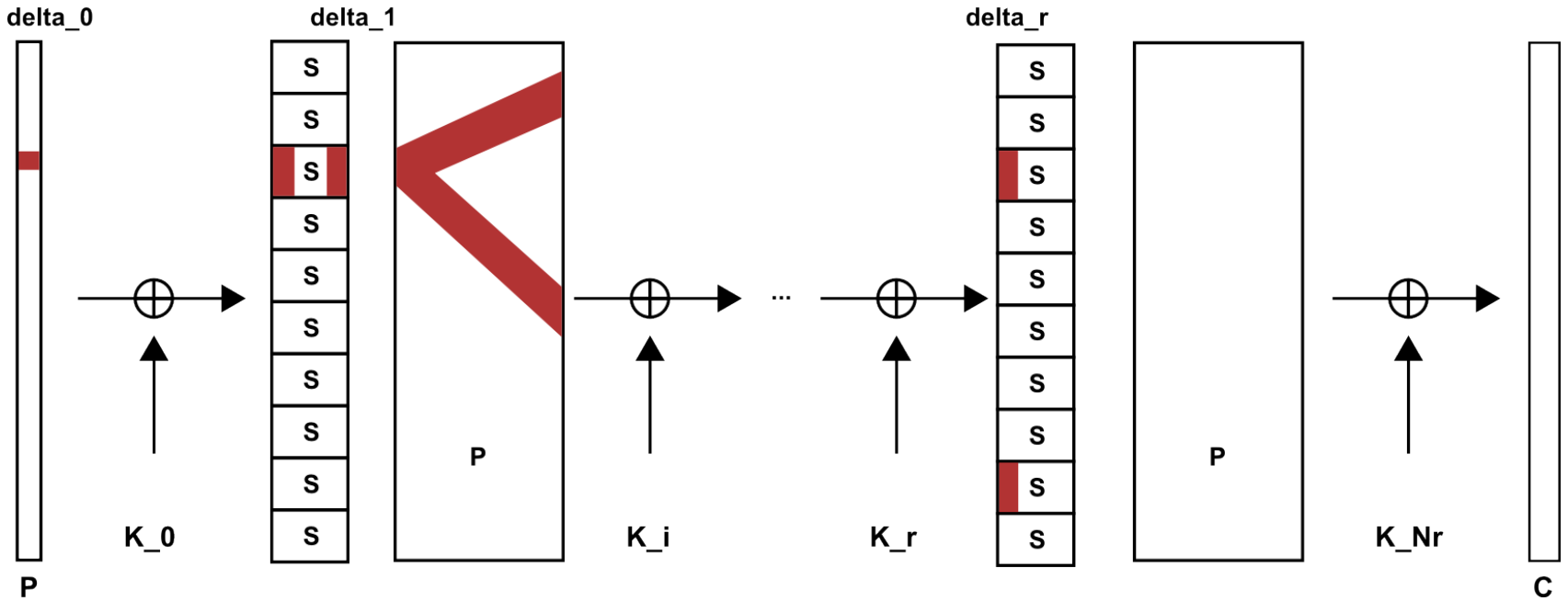


Where S is the 4-bit S-Box and P a permutation of bit positions.

Prior Attacks on Reduced Round Versions

Differential characteristics and two round filter function available in [4].

Differential Cryptanalysis I



$$Pr(\delta_i) = p_i \longrightarrow Pr(\Delta) = \prod p_i$$

Differential Cryptanalysis II

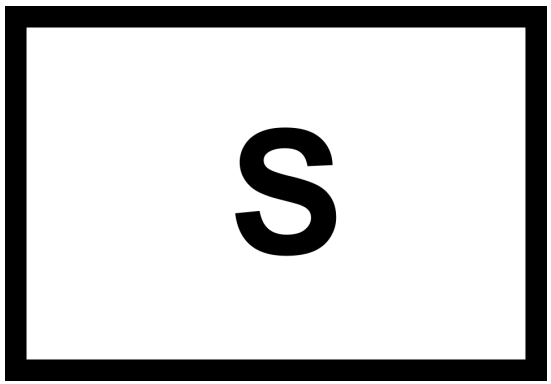
Key Recovery:

- **backward key guessing** to recover subkey bits of last rounds not covered by characteristic
- **right pairs** suggest correct and wrong key bits
- **wrong pairs** suggest random key bits
- **filter functions** used to remove wrong pairs
- **candidate key arrays** to count suggestions and observe peak

Differential Cryptanalysis of 16-round DES [1]

- distinguishes right pairs,
- uses outer round active S-Boxes to recover key bits and
- does not rely on candidate key arrays.

Algebraic Cryptanalysis



$$
\begin{aligned}
&y_2x_3 + y_3x_3 + x_1x_3 + x_2x_3 + x_3,\\
&y_0x_3 + y_3x_3 + x_1x_3 + x_2x_3 + \ldots,\\
&x_1x_2 + y_3 + x_0 + x_1 + x_3,\\
&x_0x_2 + y_3x_3 + x_1x_3 + x_2x_3 + \ldots\\
&y_3x_2 + y_3x_3 + x_1x_3 + y_0 + y_1 + y_3 \ldots\\
&y_0x_2 + y_1x_2 + y_1x_3 + y_3x_3 + \ldots\\
&x_0x_1 + y_3x_3 + x_1x_3 + x_2x_3 + \ldots\\
&y_3x_1 + y_3x_3 + x_2x_3 + \ldots, \ldots
\end{aligned}
$$

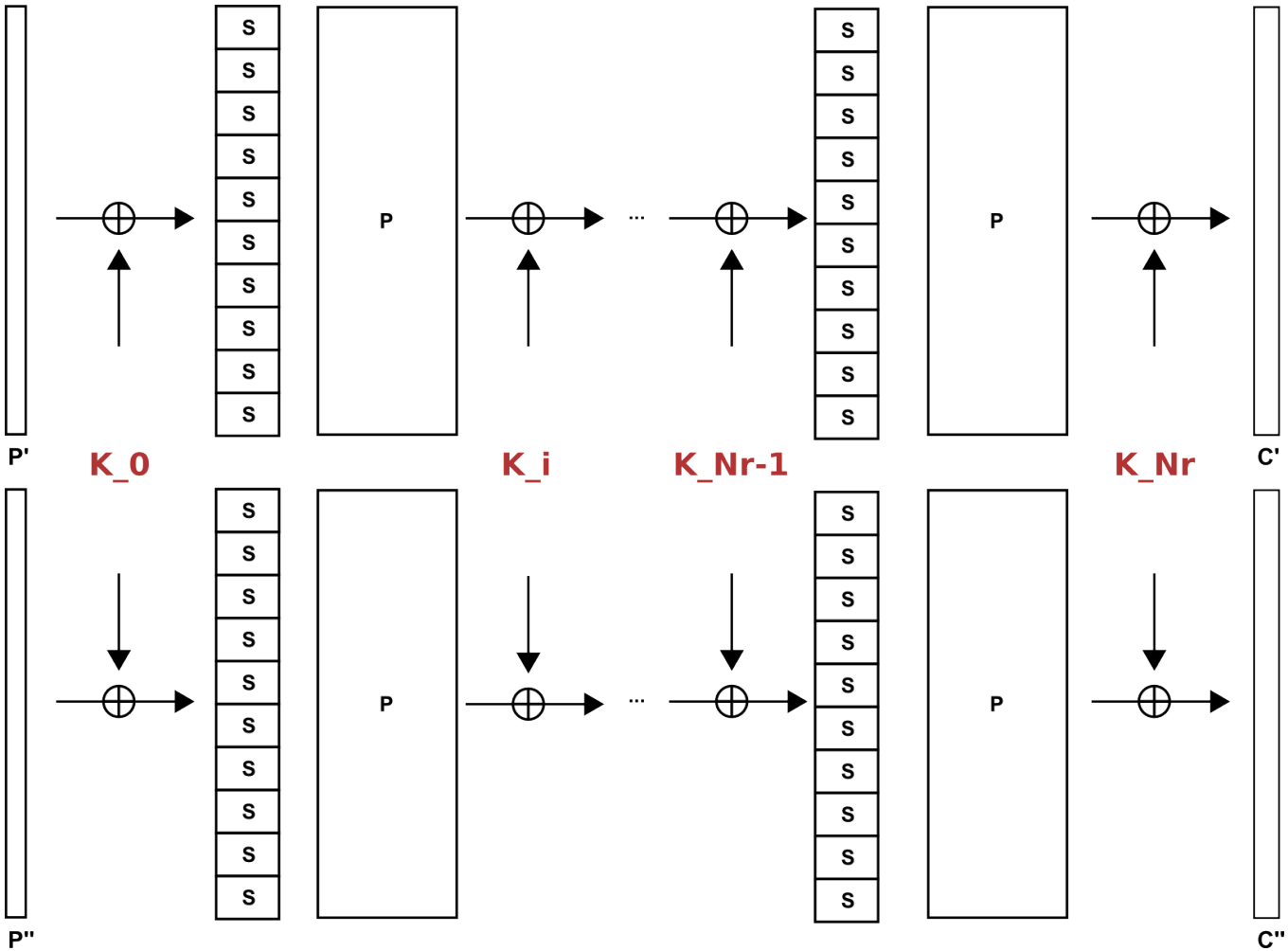
We call $X_{i,j}$ and $Y_{i,j}$ the input resp. output variable for the j-th bit of the i-th S-Box application (i.e. round).

For PRESENT-80-31 we would have a system of 8140 variables in 34742 equations if we consider two plaintext-ciphertext pairs.

Multiple $P - C$ Pairs [3] I

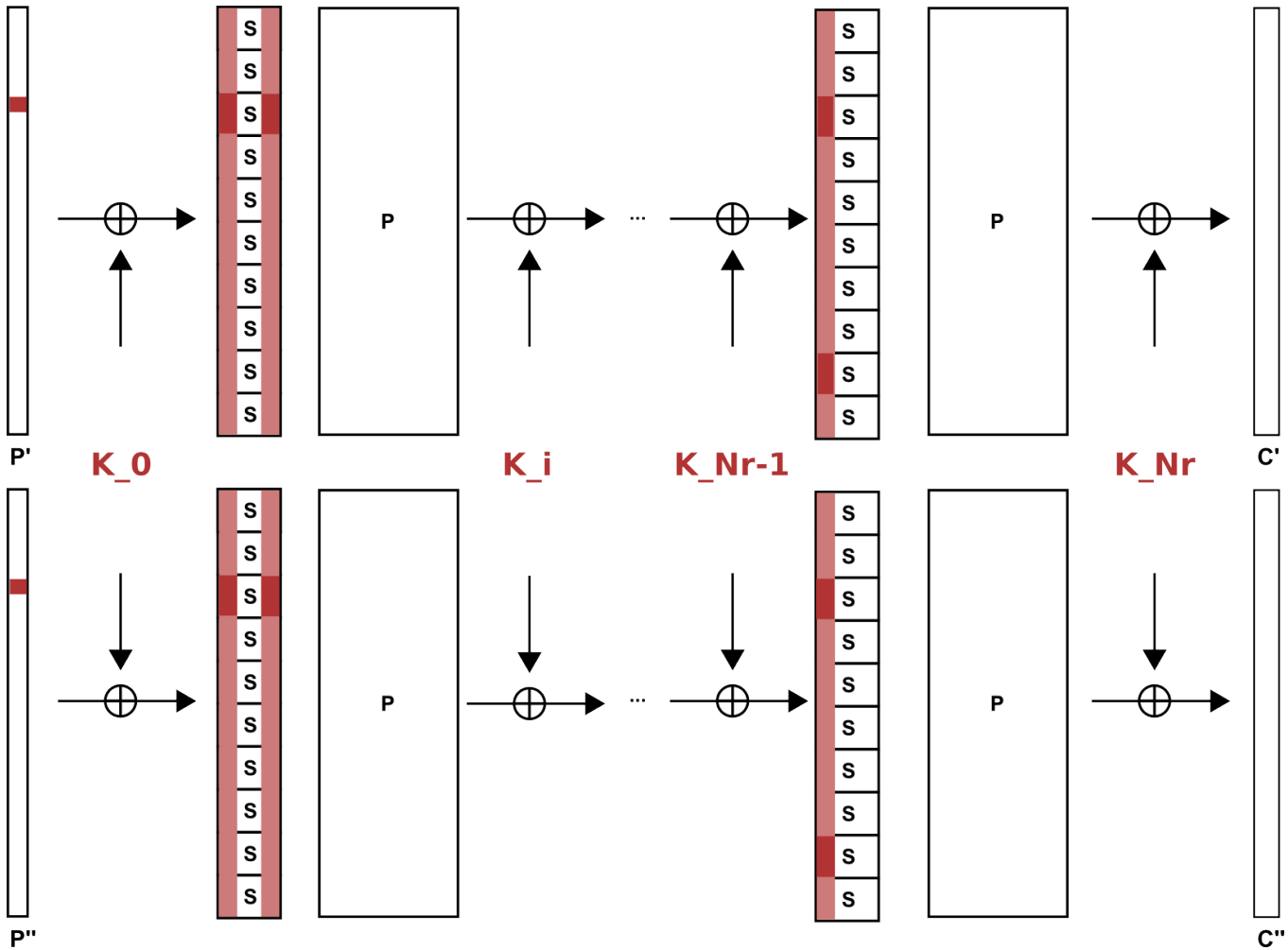
- Given two equation systems F' and F'' for two plaintext-ciphertext pairs (P', C') and (P'', C'') under same encryption key K.
- We can combine these equation systems to form a system $F = F' \cup F''$.
- While F' and F'' do not share most of the state variables X', X'', Y', Y'' but they share the key K and key schedule variables K_i.
- Thus by considering two plaintext–ciphertext pairs the cryptanalyst gathers twice as many equations, involving however many new variables.

Multiple $P - C$ Pairs [3] II



Outline

Attack-A I



Attack-A II

- Each one-round difference gives rise to equations relating the input and output pairs for active S-Boxes.
- We have that the expressions

$$X'_{j,k} + X''_{j,k} = \Delta X_{j,k} \rightarrow \Delta Y_{j,k} = Y'_{j,k} + Y''_{j,k},$$

  where $\Delta X_{j,k}, \Delta Y_{j,k}$ are known values predicted by the characteristic, are valid with some non-negligible probability p_j.
- For non-active S-Boxes we have the relations

$$X'_{j,k} + X''_{j,k} = 0 = Y'_{j,k} + Y''_{j,k}$$

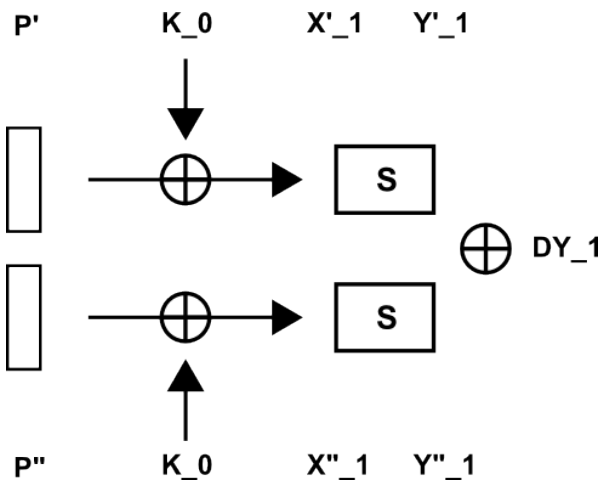
  also valid with a non-negligible probability.

These are $2n$ linear equations per round we can add to our equation system F. The resulting system $\overline{F}$ is expected to be easier to solve but we need to solve $1/p$ such systems.

Attack-B I

Restrict the first round bits to an active S-Box and assume we have a right pair. Also let the S-Box be representable by the vectorial Boolean function

$$S(X_i) = \begin{matrix} f_0(X_{i,0}, \ldots, X_{i,n-1}) \\ \ldots \\ f_{n-1}(X_{i,0}, \ldots, X_{i,n-1}) \end{matrix}.$$



If $P' - C'$ and $P'' - C''$ is a right pair, we have

- $S(P' \oplus K_0) = S(X_1') = Y_1'$
- $S(P'' \oplus K_0) = S(X_1'') = Y_1''$
- $Y_1' \oplus Y_1'' = \Delta Y_1$

$\rightarrow S(P_1' \oplus K_0) \oplus S(P_1'' \oplus K_0) = \Delta Y_1$

Attack-B II

We can use this small equation system F_s to recover bits of information about the subkey. Specifically:

Lemma

Given a differential characteristic Δ with a first round active S-Box with a difference that is true with probability 2^{-b}, then by considering F_s we can recover b bits of information about the key from this S-Box.

This is the algebraic equivalent of the well known subkey bit recovery from outer rounds as practiced in differential cryptanalysis.

In the case of PRESENT we can learn 4-bit of information per characteristic Δ.

Attack-B III

Experimental Observation

For some ciphers **Attack-A** can be used to distinguish **right pairs** and thus enables this attack.

Attack-B proceeds by measuring the time t it maximally takes to find that the system is inconsistent and assume we have a right pair if this time t elapsed without a contradiction.

Attack-B IV

N_r	K_s	r	p	SINGULAR	POLYBORI
4	80	4	2^{-16}	11.92-12.16	0.72 - 0.81
4	80	3	2^{-12}	106.55-118.15	6.18 - 7.10
4	80	2	2^{-8}	119.24-128.49	5.94 - 13.30
4	80	1	2^{-4}	137.84-144.37	11.83- **33.47**
16	80	14	2^{-62}	N/A	43.42-64.11
16	128	14	2^{-62}	N/A	45.59-65.03
16	80	13	2^{-58}	N/A	80.35-**262.73**
16	128	13	2^{-58}	N/A	81.06-320.53
16	80	12	2^{-52}	N/A	>4 hours
17	80	14	2^{-62}	12,317.49-13,201.99	55.51 - 221.77
17	128	14	2^{-62}	12,031.97-13,631.52	94.19 - 172.46
17	80	13	2^{-58}	N/A	>4 hours

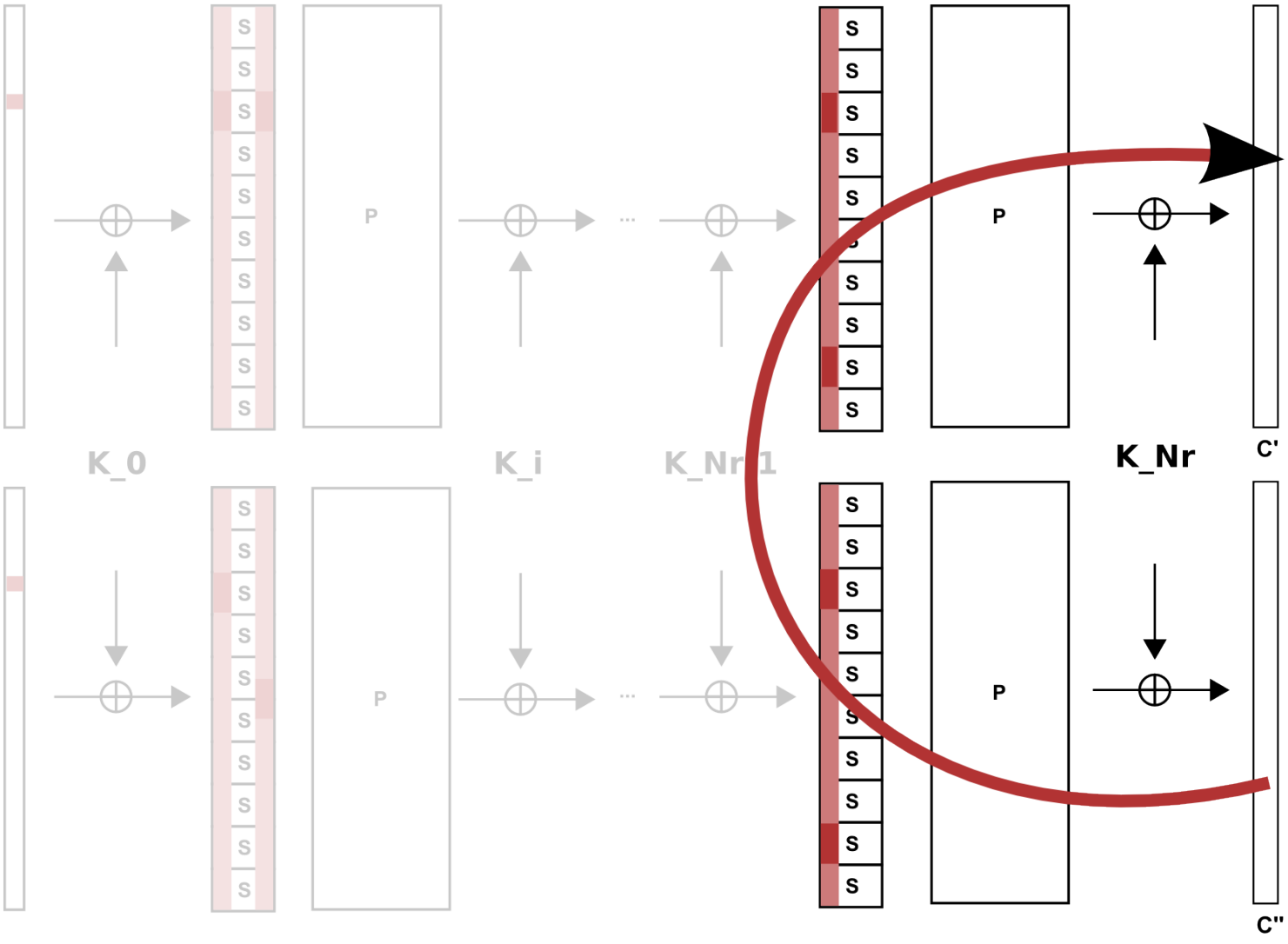
Table: Times in seconds for **Attack-B**

Times obtained on William Stein's `sage.math.washington.edu` computer purchased under NSF Grant No. 0555776.

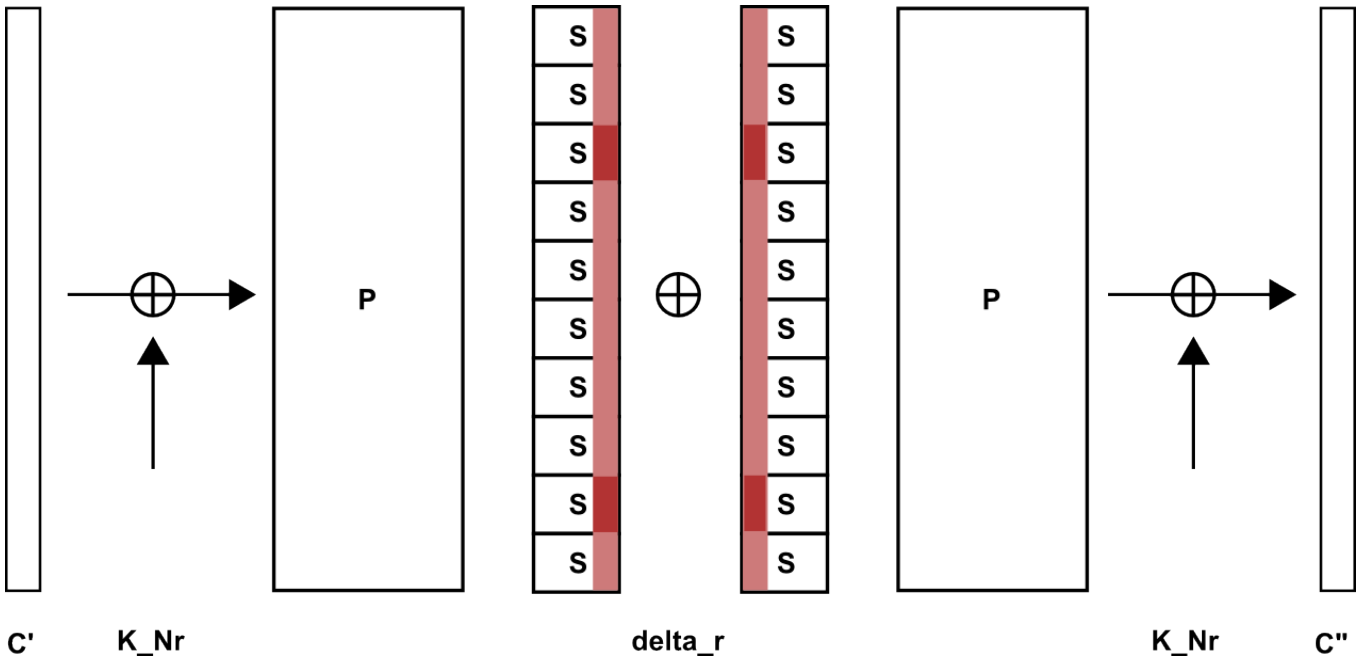
Why?

$$\frac{262.73\ s}{33.47\ s} \approx 7.85$$

Attack-C I



Attack-C II



The algebraic computation is essentially equivalent to solving a related cipher of $2(N_r - r)$ rounds (from C' to C'' via the predicted difference δ_r) with a symmetric key schedule, using an algebraic meet-in-the-middle attack.

Attack-C III

In a Nutshell

Attack-C is an algebraic filter.

Attack-C IV

N_r	r	p	#trials	K_s	t for PolyBoRi	K_s	t for PolyBoRi
4	4	2^{-16}	50	80	0.05 – 0.06	128	N/A
4	3	2^{-12}	50	80	0.88 – 1.00	128	N/A
4	2	2^{-8}	50	80	2.16 – 5.07	128	N/A
4	1	2^{-4}	50	80	8.10 – 18.30	128	N/A
16	14	2^{-62}	100	80	2.38 – 5.99	128	2.38 – 5.15
16	13	2^{-58}	100	80	8.69 – 19.36	128	9.58 – 18.64
17	14	2^{-62}	100	80	9.03 – 16.93	128	8.36 – 17.53

Table: Times in seconds for **Attack-C**

Outline

Present-80-16 I

4 bits:

- **Filter:** $(1 \pm \epsilon) \cdot 2^{62}$ ciphertext checks
- **Algebraic Filter:** $(1 \pm \epsilon) \cdot 2^{11.93} \cdot 6 \cdot 1.8 \cdot 10^9 \approx 2^{46}$ cpu cycles

Full Key Recovery:

- **Characteristics:** 6 characteristics from [5]
- **Filter:** $6 \cdot (1 \pm \epsilon) \cdot 2^{62}$ ciphertext checks
- **Algebraic Filter:** $6 \cdot (1 \pm \epsilon) \cdot 2^{46}$ cpu cycles
- **Guess:** $80 - 18 = 62$ bits

Present-128-18

Consider the input difference for round 15 and iterate over all possible output differences. For the exampel difference we have 36 possible output differences for round 15.

Full Key Recovery:

- **Algebraic Filter:** $6 \cdot (1 \pm \epsilon) \cdot 36 \cdot 2^{62} \cdot 18 \cdot 1.8 \cdot 10^9 \approx 2^{102}$ cpu cycles
- **Guessing:** $128 - 18 = 110$ bits

Experimental Results Summary

Attack	N_r	K_s	r	#pairs	time	#bits	$K_s - \#bits$
Wang	16	80	14	2^{63}	2^{65} MA	57	23
Attack-C	16	80	14	2^{62}	2^{62} MA	4	76
Attack-C	16	80	14	$6 \cdot 2^{62}$	2^{62} encr.	18	62
Attack-C	18	128	14	2^{62}	2^{102} cycles	4	124
Attack-C	18	128	14	$6 \cdot 2^{62}$	2^{110} encr.	128	110

Outline

Discussion

Properties:

- One right pair is sufficient to learn some information about the key.
- No requirement for candidate key counter.
- Silimar to DC attack on full DES [1] but **in theory** applicable to any block cipher.

Open problems:

- Is this idea applicable to other ciphers?
- How long would it take to solve the small cipher system in Attack-C after a right pair has been identified?
- Can we use the statistical filter to improve the algebraic filter directly rather than prefixing it?

Conclusion

- We presented a new approach which uses algebraic techniques in differential cryptanalysis.
- Specifically, we show how to invest more time in the last rounds not covered by a differential.
- To illustrate the viability of the attack we improved the best known attack against PRESENT-128 by two rounds using the same characteristics.

Note

This attack has no implication for the security of PRESENT!

Thank you!

Literature I


E. Biham and A. Shamir.
Differential Cryptanalysis of the Full 16-round DES.
In *Advances in Cryptology — CRYPTO 1992*, volume 740 of *LNCS*, pages 487–496. Springer, 1991.


A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, Matthew Robshaw, Y. Seurin, and C. Vikkelsoe.
PRESENT: An ultra-lightweight block cipher.
In *CHES 2007*, volume 7427 of *LNCS*, pages 450–466. Springer, 2007.


Jean-Charles Faugère.
Groebner bases. Applications in cryptology.
FSE 2007 - Invited Talk.
available at `http://fse2007.uni.lu/v-misc.html`.

Literature II


M. Wang.
Differential cryptanalysis of PRESENT.
Cryptology ePrint Archive, Report 2007/408, 2007.
http://eprint.iacr.org/2007/408.


M. Wang.
Private communication: 24 differential characteristics for 14-round present, 2008.