Algebraic Techniques in Differential Cryptanalysis

. . . walking that extra mile with algebra

Martin Albrecht[1]

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

Egham, 21. Februrary 2008

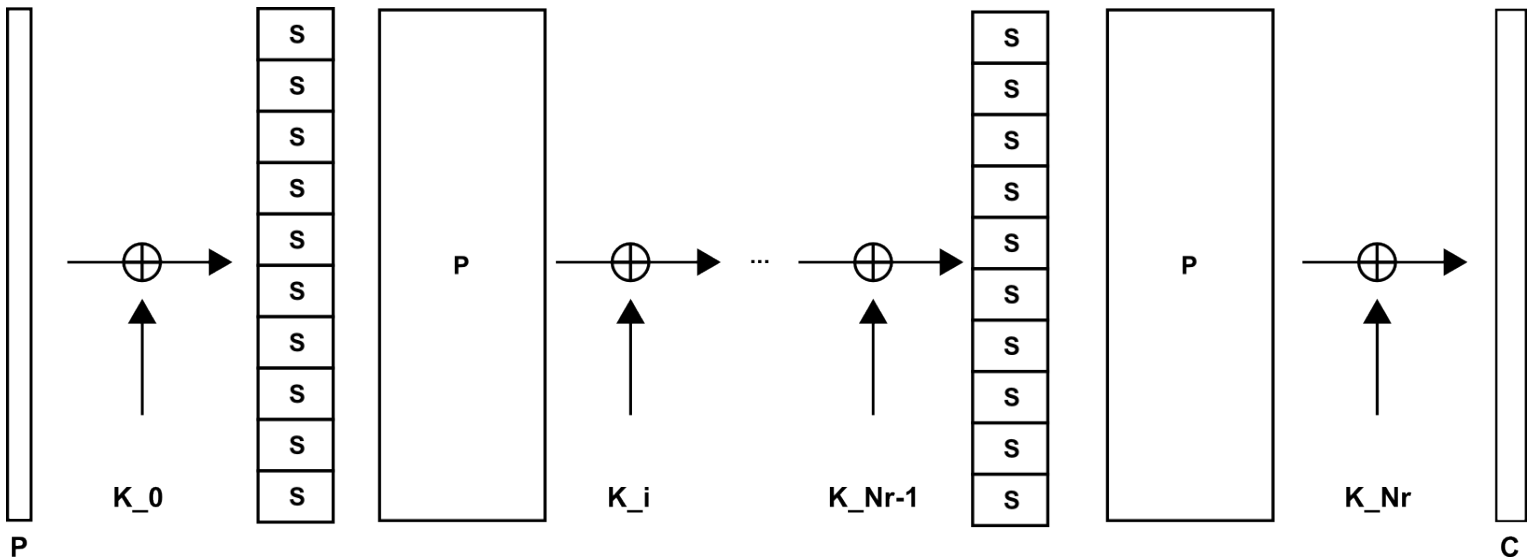
[1] joint work with Carlos Cid

Outline

Outline

The Blockcipher PRESENT

PRESENT [4] was proposed by Bogdanov et al. at CHES 2007 as an ultra-lightweight block cipher, suitable for RFIDs and similar devices.



Where the S-Box is defined as

$$S = [12, 5, 6, 11, 9, 0, 10, 13, 3, 14, 15, 8, 4, 7, 1, 2]$$

and the permutation layer P as $4 \cdot j + i \rightarrow 16 \cdot i + j$ with $(0 \leq j < 16, 0 \leq i < 4)$.

PRESENT-80 Key Schedule

The user-supplied key is stored in key register K and represented as

$$K = k_{79}k_{78}\ldots k_0.$$

At round i the round key K_i consists of the 64 most significant bits of K.

$$K_i = k_{i,63}k_{i,62}\ldots k_{i,0} = k_{79}k_{78}\ldots k_{16}.$$

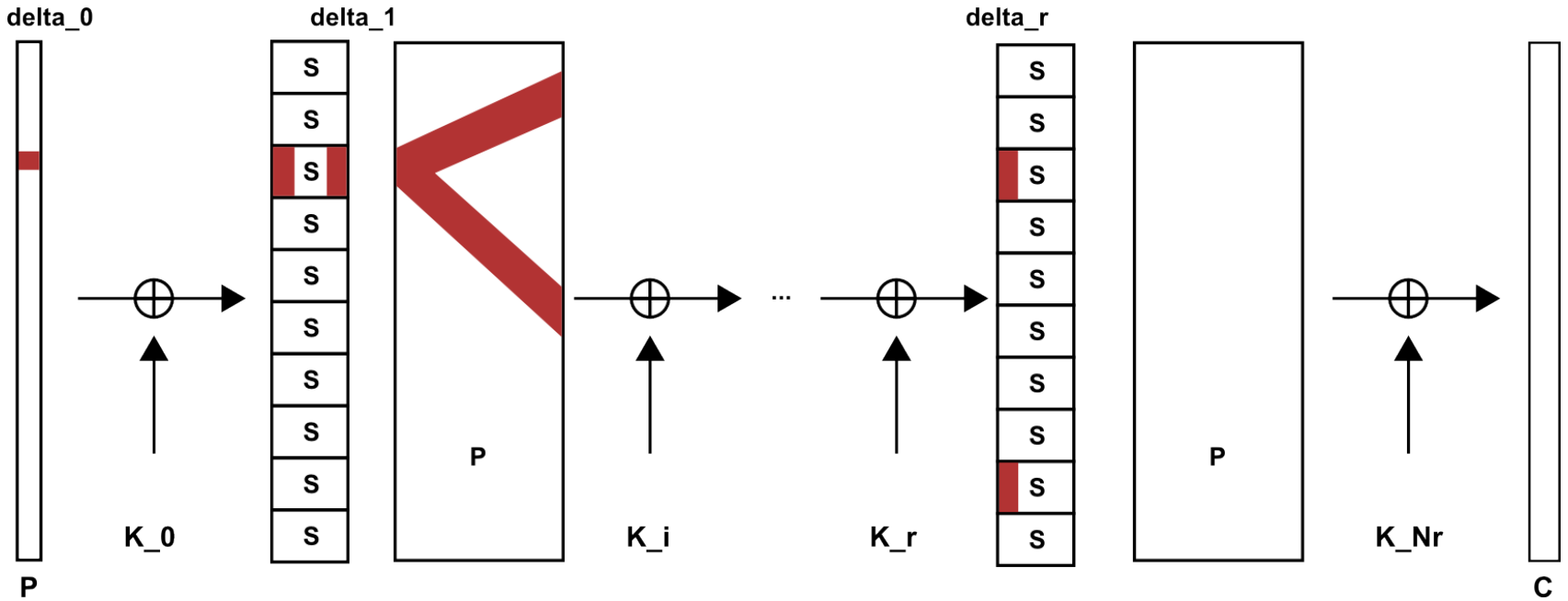
Afterwards, the key register is updated:

1. $[k_{79}k_{78}\ldots k_1k_0] = [k_{18}k_{17}\ldots k_{20}k_{19}]$
2. $[k_{79}k_{78}k_{77}k_{76}] = \mathbf{S}[\mathbf{k_{79}k_{78}k_{77}k_{76}}]$
3. $[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15}] \oplus \text{round\_counter}$

The key schedule for 128-bit keys is quite similar.

Outline

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 III

Properties of the attack:

- One of the most successful attack techniques against block ciphers, hash functions, etc. [2].
- Usually requires huge quantities of plaintext–ciphertext pairs ($> 2^{-p}$).
- Attack is well understood, so modern block ciphers usually do not have their security affected.

Differential Cryptanalysis of 16-round DES [3]

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

Difference Distribution Matrix for PRESENT

$$
\begin{pmatrix}
16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 4 & 0 & 0 & 0 & 4 & 0 & 0 \\
0 & 0 & 0 & 2 & 0 & 4 & 2 & 0 & 0 & 0 & 2 & 0 & 2 & 2 & 2 & 0 \\
0 & 2 & 0 & 2 & 2 & 0 & 4 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 4 & 2 & 2 & 0 & 2 & 2 & 0 & 2 & 0 & 2 & 0 \\
0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 4 & 2 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 4 & 2 & 0 & 0 & 4 \\
0 & 4 & 2 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 4 \\
0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 4 & 0 & 2 & 0 & 4 \\
0 & 0 & 2 & 0 & 4 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 4 & 0 \\
0 & 0 & 2 & 2 & 0 & 4 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 2 & 2 & 0 \\
0 & 2 & 0 & 0 & 2 & 0 & 0 & 0 & 4 & 2 & 2 & 2 & 0 & 2 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 4 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 0 & 2 & 0 \\
0 & 2 & 4 & 2 & 2 & 0 & 0 & 2 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 2 & 2 & 0 & 0 & 2 & 2 & 0 & 0 \\
0 & 4 & 0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4
\end{pmatrix}
$$

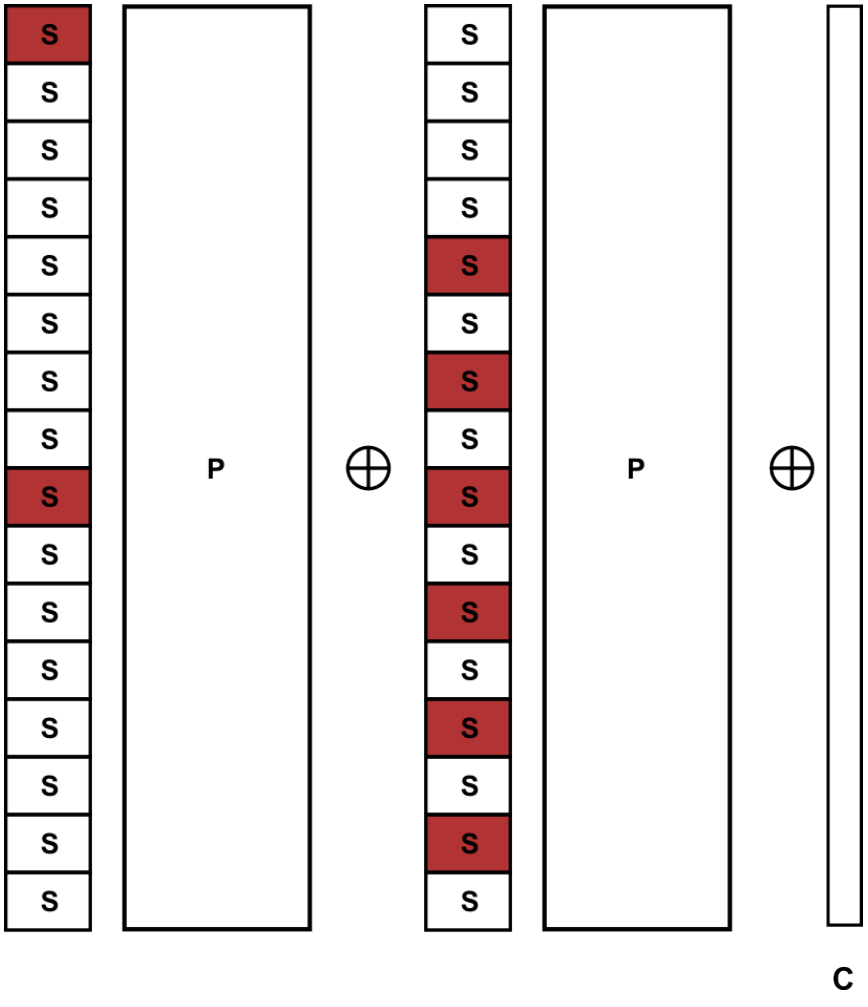
$$
Pr(\Delta X = 1 \rightarrow \Delta Y = 3) = \frac{4}{16} = \frac{1}{4}
$$

14-Round Characteristic for PRESENT [12]

Rounds		Differences	Pr	Rounds		Difference	Pr
I		$x_2 = 7, x_{14} = 7$	1				
R1	S	$x_2 = 1, x_{14} = 1$	2^{-4}	R8	S	$x_8 = 9, x_{10} = 9$	2^{-4}
R1	P	$x_0 = 4, x_3 = 4$	1	R8	P	$x_2 = 5, x_{14} = 5$	1
R2	S	$x_0 = 5, x_3 = 5$	2^{-4}	R9	S	$x_2 = 1, x_{14} = 1$	2^{-6}
R2	P	$x_0 = 9, x_8 = 9$	1	R9	P	$x_0 = 4, x_3 = 4$	1
R3	S	$x_0 = 4, x_8 = 4$	2^{-4}	R10	S	$x_0 = 5, x_3 = 5$	2^{-4}
R3	P	$x_8 = 1, x_{10} = 1$	1	R10	P	$x_0 = 9, x_8 = 9$	1
R4	S	$x_8 = 9, x_{10} = 9$	2^{-4}	R11	S	$x_0 = 4,\ x_8 = 4$	2^{-4}
R4	P	$x_2 = 5, x_{14} = 5$	1	R11	P	$x_8 = 1,\ x_{10} = 4$	1
R5	S	$x_2 = 1, x_{14} = 1$	2^{-6}	R12	S	$x_8 = 9,\ x_{10} = 9$	2^{-4}
R5	P	$x_0 = 4, x_3 = 4$	1	R12	P	$x_2 = 5,\ x_{14} = 5$	1
R6	S	$x_0 = 5, x_3 = 5$	2^{-4}	R13	S	$x_2 = 1,\ x_{14} = 1$	2^{-6}
R6	P	$x_0 = 9, x_8 = 9$	1	R13	P	$x_0 = 4,\ x_3 = 4$	1
R7	S	$x_0 = 4, x_8 = 4$	2^{-4}	R14	S	$x_0 = 5,\ x_3 = 5$	2^{-4}
R7	P	$x_8 = 1, x_{10} = 1$	1	R14	P	$x_0 = 9,\ x_8 = 9$	1

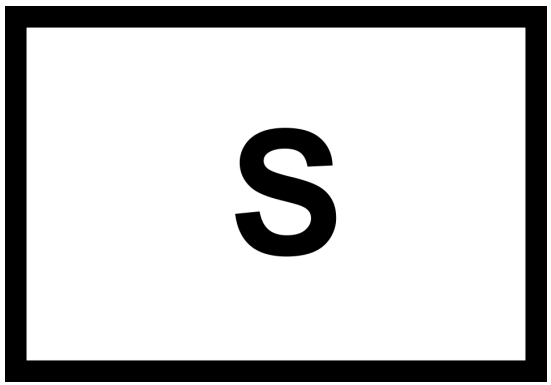
Table: 14-round differential characteristic for PRESENT with probability 2^{-62}

Two Round Filter Function for PRESENT-80-16 [12]



- Two S-Boxes are active in round 15.
- Each has six possible output differences.
- We have 36 possible output differences for round 15.
- At most 6 S-Boxes are active in round 16.
- We can discard $\sim 2^{50}$ out of 2^{62} pairs.

Algebraic Cryptanalysis I



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

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.

Algebraic Cryptanalysis II

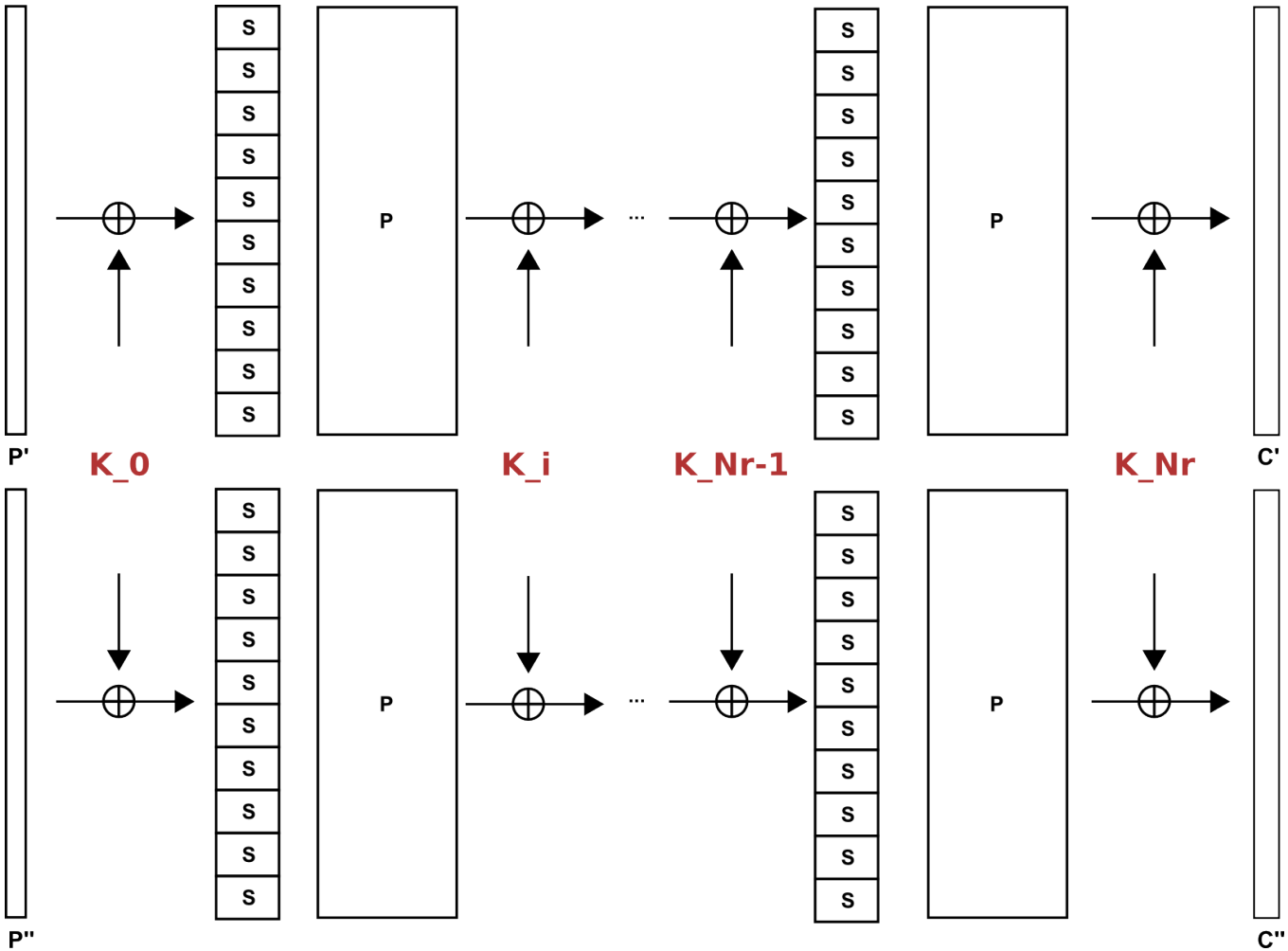
Properties of the attack:

- Requires very few plaintext–ciphertext pairs (~ 1).
- No attack against "industrial strength" cipher faster than other techniques known.
- Algorithms: Bucherberger algorithm [7], F_4 [9], F_5 [10], Raddum-Semaev [11], SAT-solvers [1], XL family [6]
- Often statistical components: SAT-solvers, key bit guessing, AES inversion equations $xy + 1$ [5].

Multiple $P - C$ Pairs [8] I

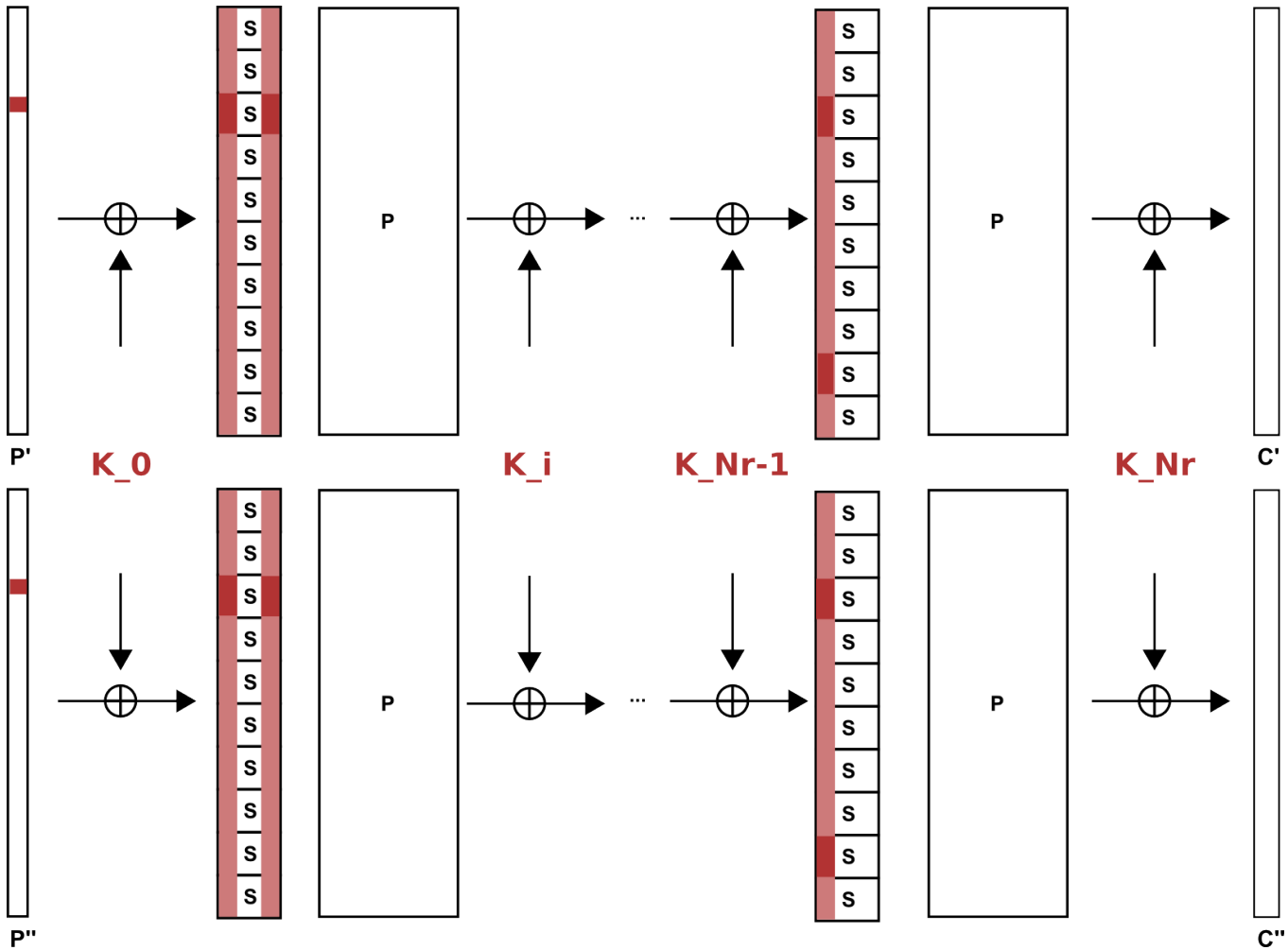
- Given two equation systems F' and F'' for two plaintext-ciphertext pairs (P', C') and (P'', C'') under same encryption key K.
- We can combine these equation systems to form a system $F = F' \cup F''$.
- While F' and F'' do not share most of the state variables X', X'', Y', Y'' but they share the key 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 [8] 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

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

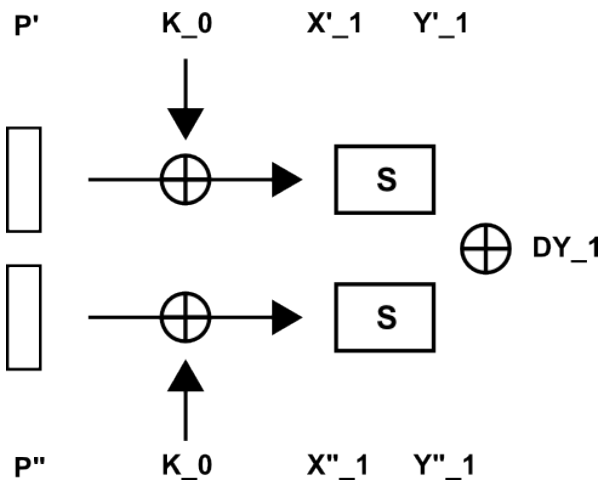
  also valid with a non-negligible probability.

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.

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

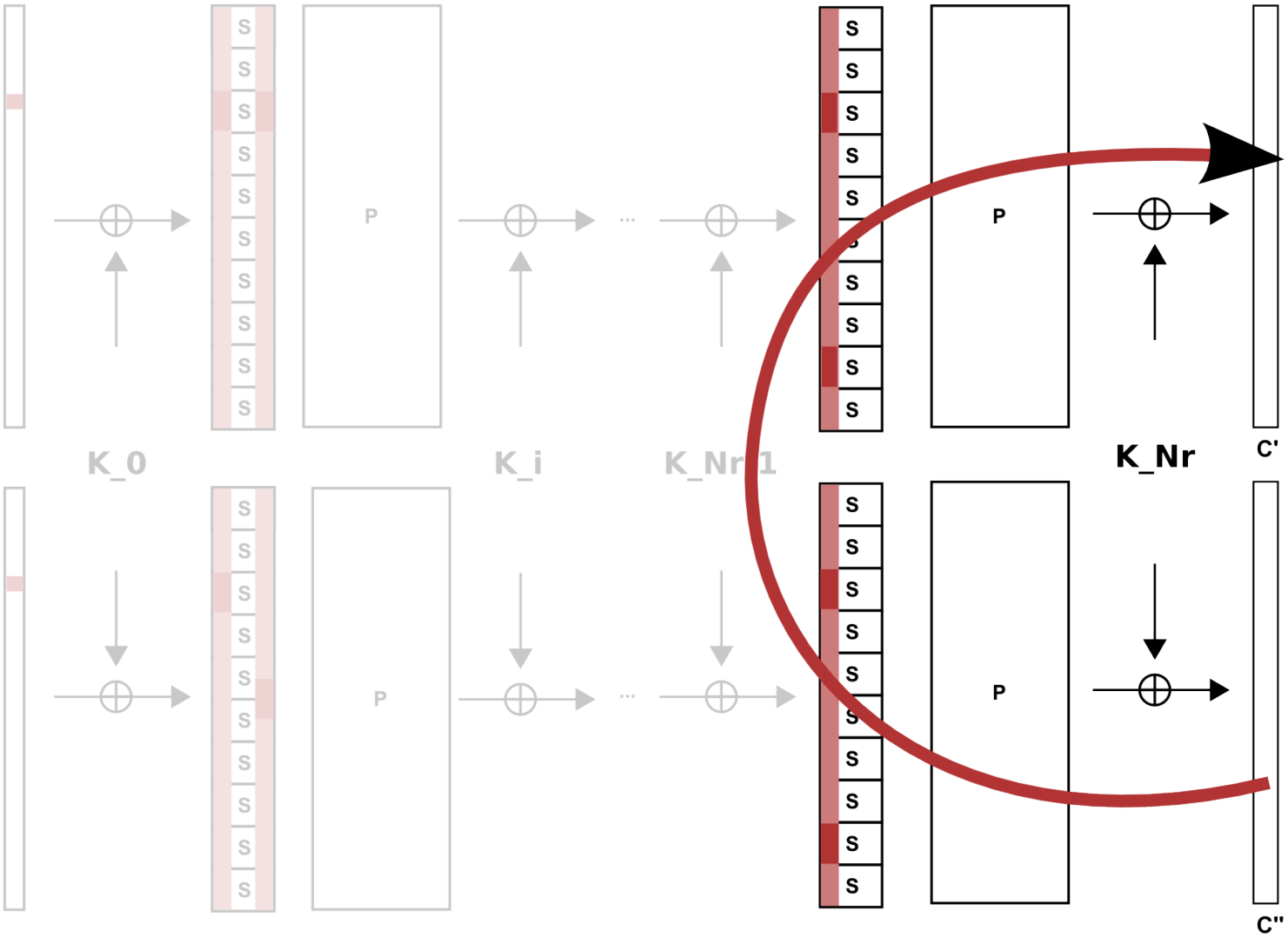
Table: Times in seconds for **Attack-B**

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

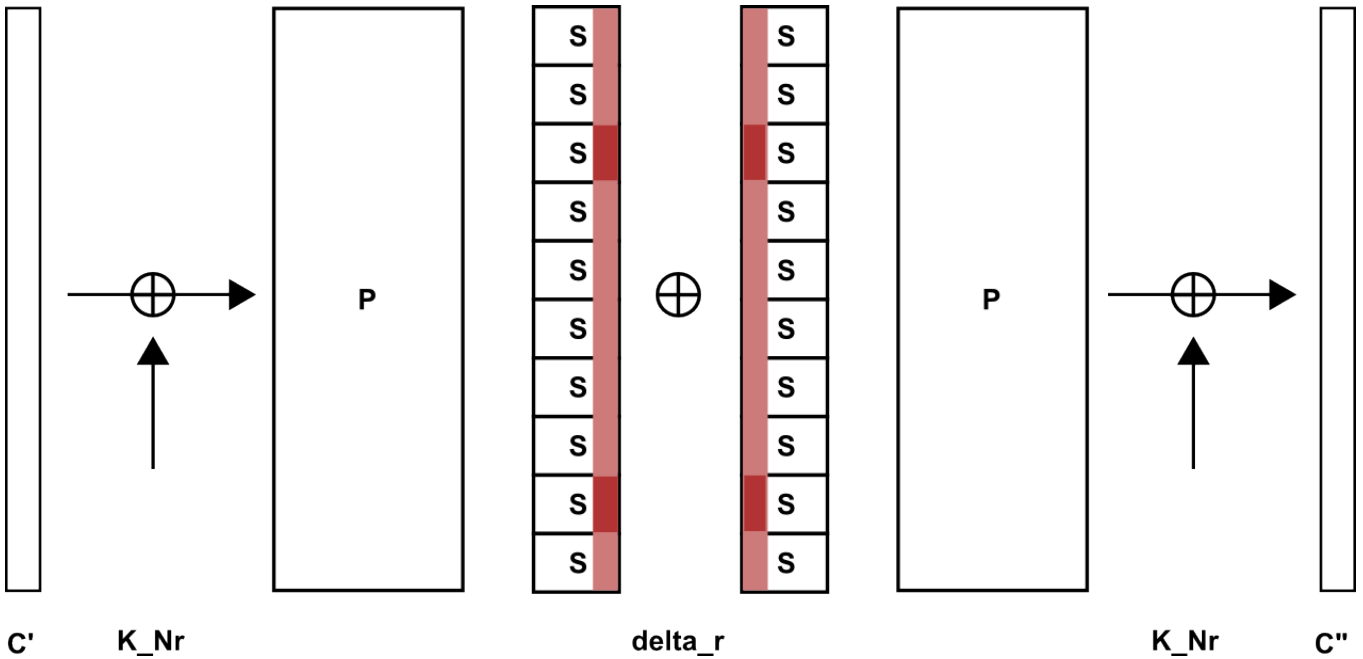
Why?

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

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 [13]
- **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 [3] but **in theory** applicable to any block cipher.

Possible improvements are

- better algebraic representations,
- better algorithms (e.g. SAT-solvers) and
- better exploitation of right pair.

PRESENT-128-(18+i)?

Speculation

It might be possible to find contradictions using **Attack-C** in $\ll 2^{128-62} = 2^{66}$ cpu cycles for PRESENT-128-20 "a situation without precedent" [4].

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

Gregory V. Bard.
Algorithms for Solving Linear and Polynomial Systems of Equations over Finite Fields with Applications to Cryptanalysis.
PhD thesis, 2007.
available at
`http://www.cs.umd.edu/~jkatz/THESES/bard_thesis.pdf`.

E. Biham and A. Shamir.
Differential Cryptanalysis of DES-like Cryptosystems.
In *Advances in Cryptology — CRYPTO 1990*, volume 537 of *LNCS*, pages 3–72. Springer, 1991.

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.

Literature II


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.


Carlos Cid, Sean Murphy, and Matthew Robshaw.
Algebraic Aspects of the Advanced Encryption Standard.
Springer, 2006.


Nicolas T. Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir.
Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations.
In *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 392–407. Springer, 2000.

Literature III


David Cox, John Little, and Donal O'Shea.
Ideals, Varieties, and Algorithms.
Springer, 2005.


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


Jean-Charles Faugère.
A New Efficient algorithm for Computing Gröbner Basis (F4), 1999.
available at
`http://modular.ucsd.edu/129-05/refs/faugere_f4.pdf`.


Jean-Charles Faugère.
A New Efficient Algorithm for Computing Gröbner Bases without Reduction to Zero (F5).
In *Proceedings of ISSAC*, pages 75–83. ACM Press, 2002.

Literature IV


Havard Raddum and Igor Semaev.
New technique for solving sparse equation systems.
Cryptology ePrint Archive, Report 2006/475, 2006.
available at http://eprint.iacr.org/2006/475.


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.