Cryptanalysis of KLEIN

FSE 2014

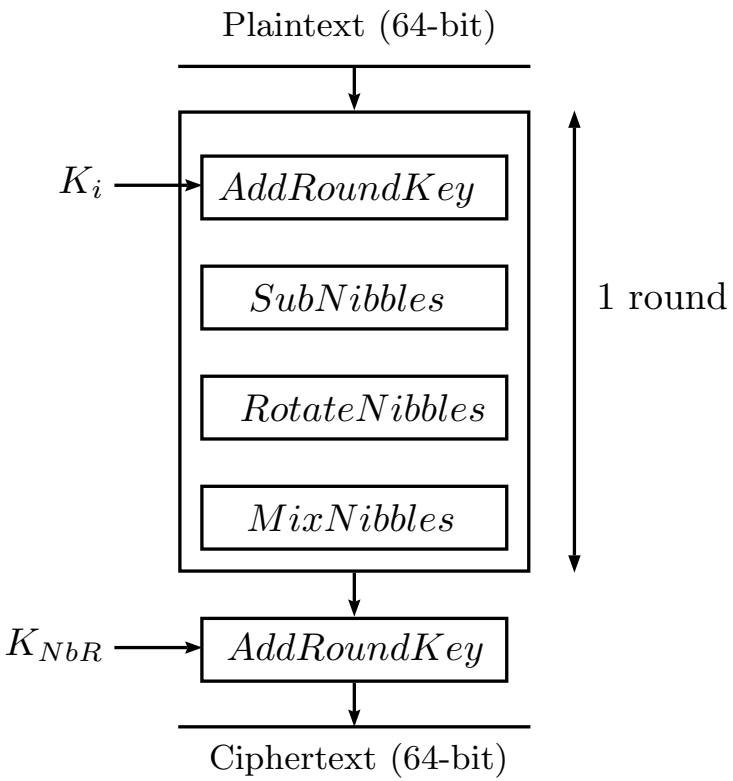
Virginie Lallemand and María Naya-Plasencia

Inria, France

March 4th 2014

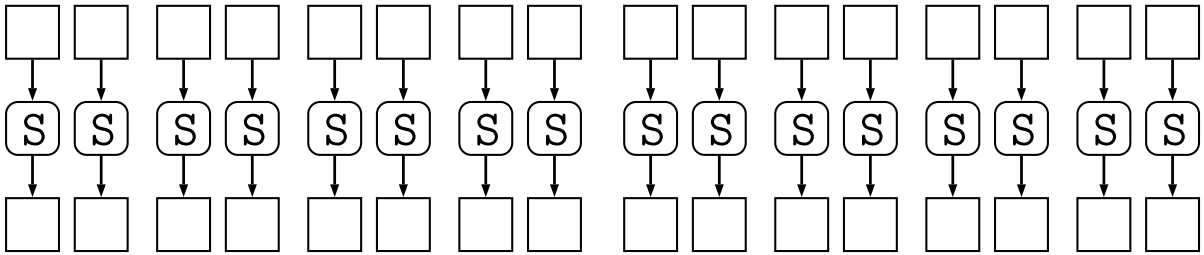
The KLEIN Block Cipher

Family of Lightweight Block Ciphers presented at RFIDSec 2011 by Zheng Gong, Svetla Nikova, and Yee Wei Law



Version	Key Size	Rounds
KLEIN-64	64	12
KLEIN-80	80	16
KLEIN-96	96	20

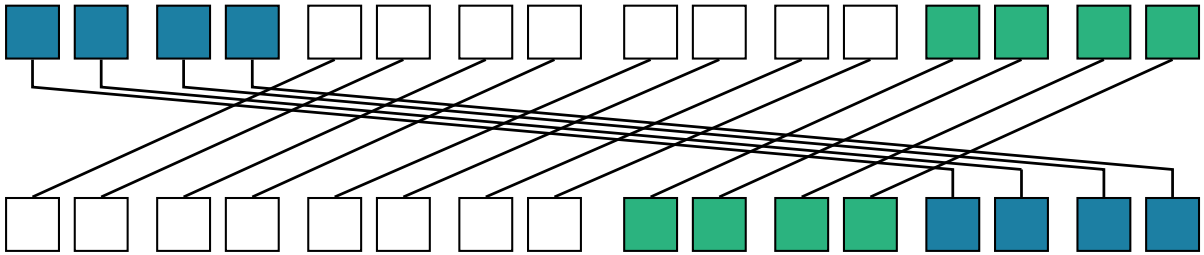
SubNibbles (SN)



Splits the state into 4-bit parts (nibbles) and applies the following Sbox:

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S[x]	7	4	a	9	1	f	b	0	c	3	2	6	8	e	d	5

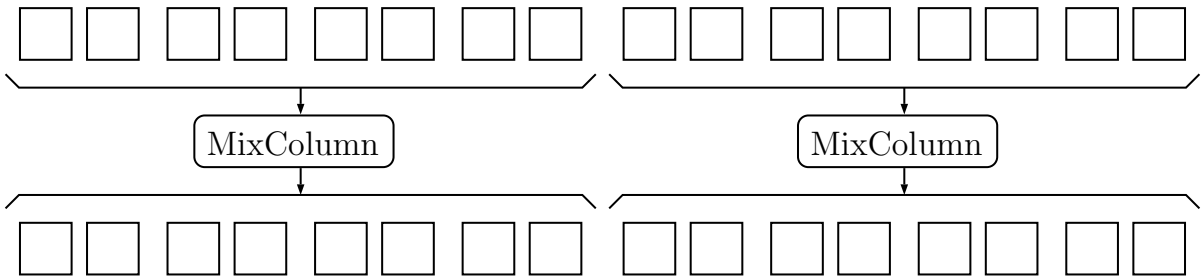
RotateNibbles (RN)



Cyclic rotation of the state leftwards by 2 bytes / 4 nibbles.

MixNibbles (MN)

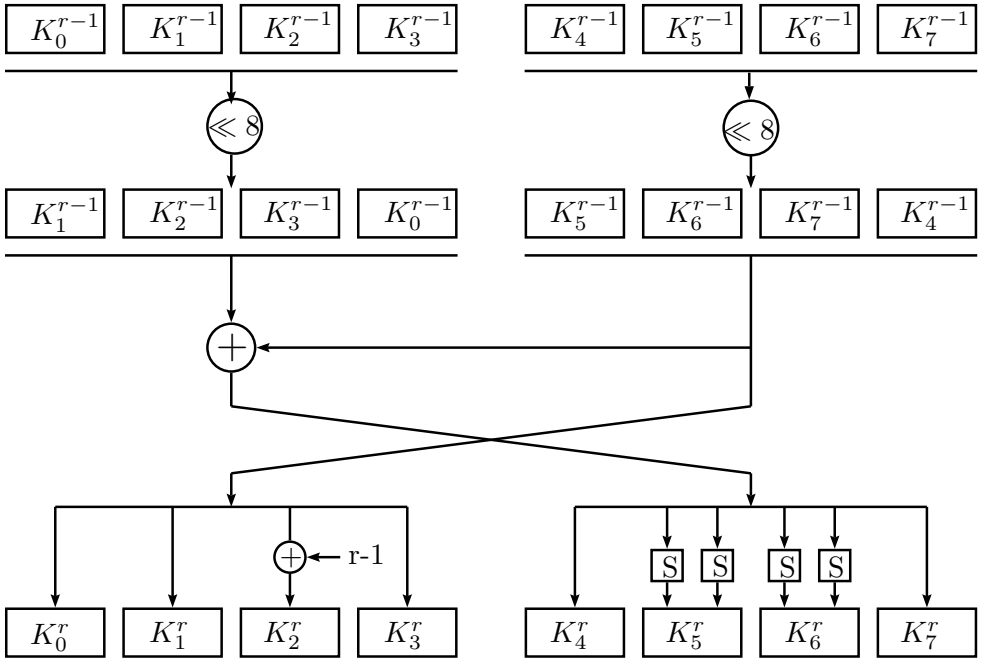
Byte wise operation computing AES `MixColumn` transformation on each half of the state



A byte is seen as an element of $GF(2^8) = GF(2)/x^8 + x^4 + x^3 + x + 1$
The output is composed of 4 bytes resulting from multiplication with the following matrix:

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

Key-Schedule (KLEIN-64)



Main Idea of Previous Analyses

Main Idea of Previous Analyses

proposition [ANS 11][YWLZ 11]

During encryption and key derivation, there is a slow diffusion between higher and lower nibbles.

Main Idea of Previous Analyses

proposition [ANS 11][YWLZ 11]

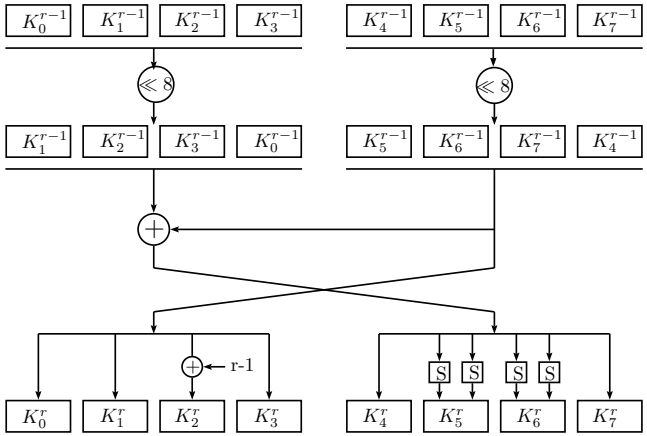
During encryption and key derivation, there is a slow diffusion between higher and lower nibbles.

Version	Attacks	Rounds	Data	Time	Memory	Source
KLEIN-64	integral	7	$2^{34.3}$	$2^{45.5}$	2^{32}	[YWLZ 11]
	truncated	8	2^{32}	$2^{46.8}$	2^{16}	[YWLZ 11]
	differential	8	2^{35}	2^{35}	-	[ANS 11]
	PC MITM	10	1	2^{62}	2^{60}	[NWW 13]
	biclique	12	2^{39}	$2^{62.84}$	$2^{4.5}$	[ASR 13]
KLEIN-80	integral	8	$2^{34.3}$	$2^{77.5}$	2^{32}	[YWLZ 11]
	PC MITM	11	2	2^{74}	2^{74}	[NWW 13]
	biclique	16	2^{48}	2^{79}	2^{60}	[AFLLW 12]
KLEIN-96	PC MITM	13	2	2^{94}	2^{82}	[NWW 13]
	biclique	20	2^{32}	$2^{95.18}$	2^{60}	[AFLLW 12]

Properties

proposition [ANS 11][YWLZ 11]

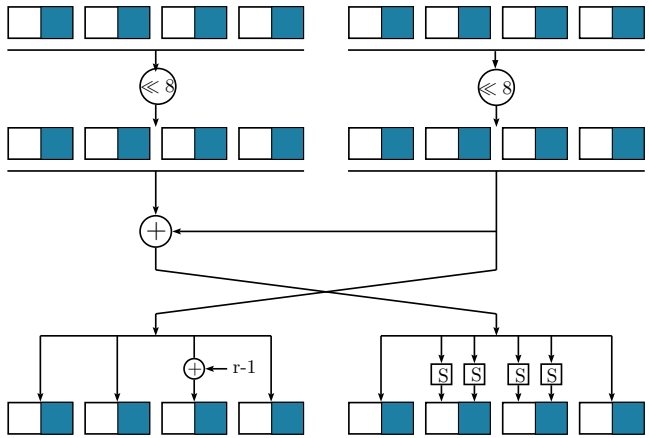
In the `KeySchedule` algorithm, lower nibbles and higher nibbles are not mixed: the lower nibbles (resp. higher nibbles) of any round-key can be computed directly from the lower nibbles (resp. higher nibbles) of the master key.



Properties

proposition [ANS 11][YWLZ 11]

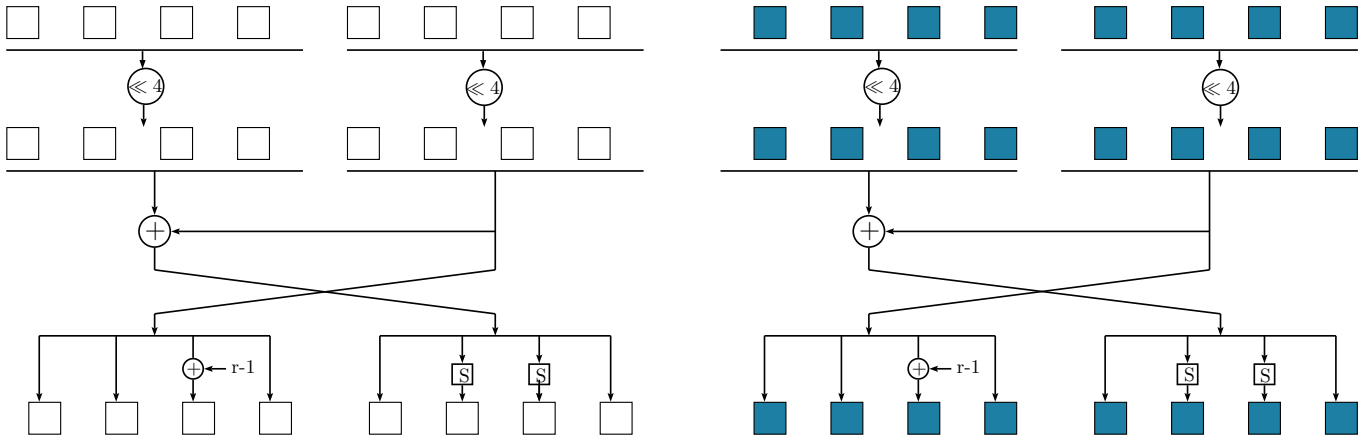
In the `KeySchedule` algorithm, lower nibbles and higher nibbles are not mixed: the lower nibbles (resp. higher nibbles) of any round-key can be computed directly from the lower nibbles (resp. higher nibbles) of the master key.



Properties

proposition [ANS 11][YWLZ 11]

In the `KeySchedule` algorithm, lower nibbles and higher nibbles are not mixed: the lower nibbles (resp. higher nibbles) of any round-key can be computed directly from the lower nibbles (resp. higher nibbles) of the master key.



Properties

proposition [ANS 11][YWLZ 11]

All layers except `MixNibbles` are nibble-wise and do not mix higher nibbles with lower nibbles.

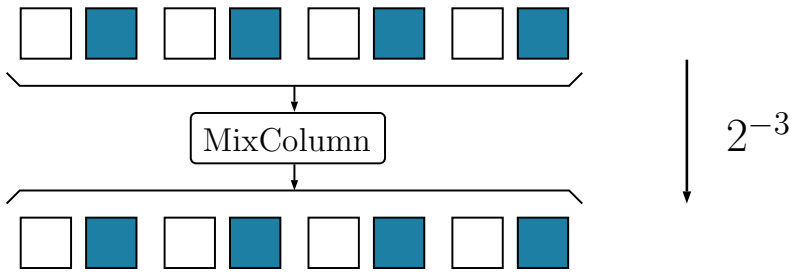
Properties

proposition [ANS 11][YWLZ 11]

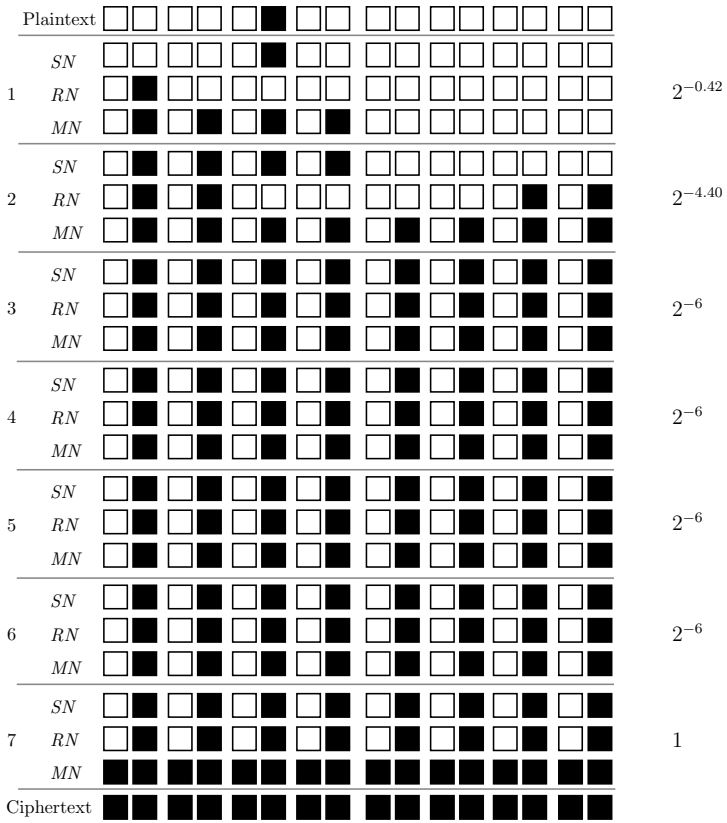
All layers except `MixNibbles` are nibble-wise and do not mix higher nibbles with lower nibbles.

proposition [ANS 11][YWLZ 11]

If the state entering `MixColumn` has inactive higher nibbles, then the output has the same pattern if and only if the MSB of the 4 lower nibble differences all have the same value. This case occurs with probability 2^{-3}. The same property holds for $\texttt{MixColumn}^{-1}$

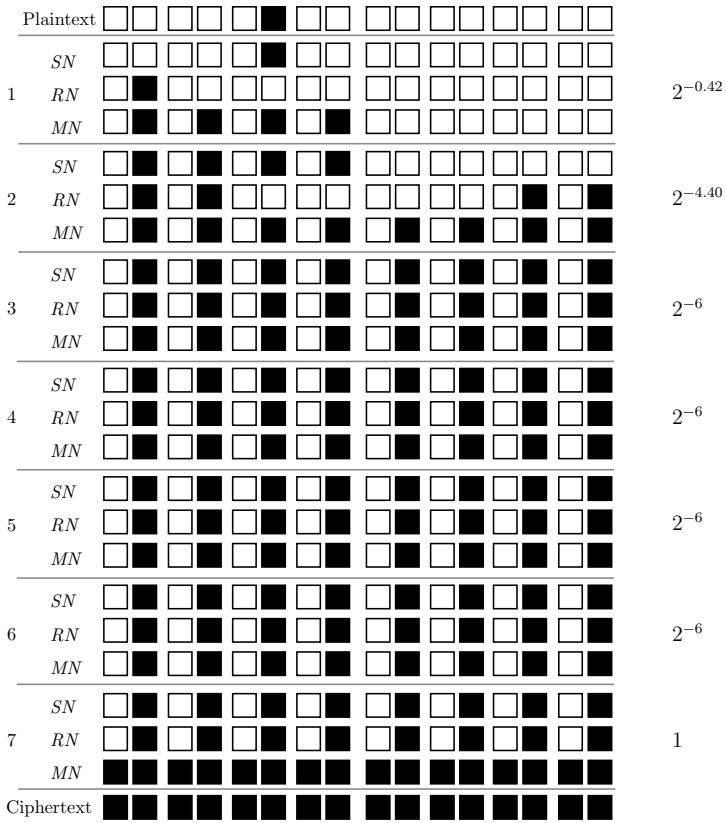


Resulting Truncated Differential Attack [ANS 11]



- Probability $2^{-28.82}$
- Find several conforming pairs
- Use the difference before MN at round 6 to reduce the key space (2^{-6})

Resulting Truncated Differential Attack [ANS 11]



- Probability $2^{-28.82}$
- Find several conforming pairs
- Use the difference before MN at round 6 to reduce the key space (2^{-6})

If we try to attack more rounds:

- Hard to filter conforming pairs
- Expensive to get several ones

New Attack

New Attack

Principle

Access MN of the previous rounds to obtain bigger sieves

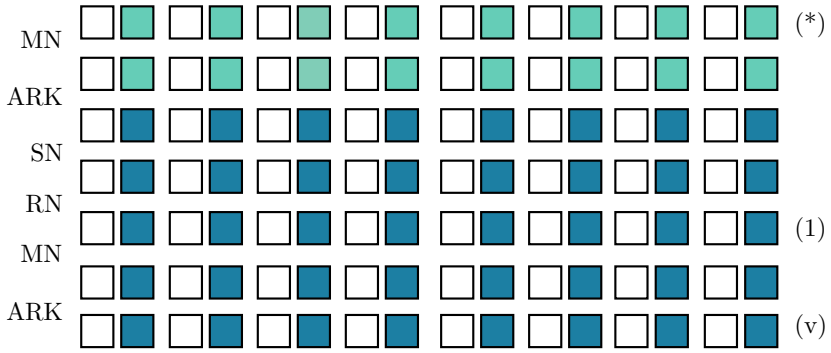
New Attack

Principle

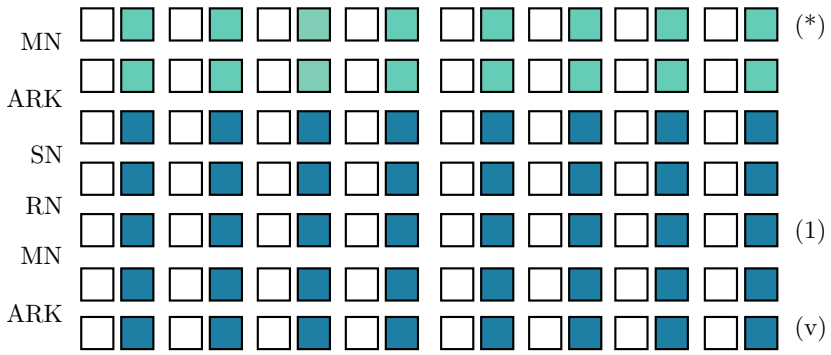
Access MN of the previous rounds to obtain bigger sieves

- Build triples made up of 2 messages and a possible value for the lower nibbles of the master key
- Test together if the key guess is correct and if the pair is conforming to the differential path
- Invert a round to access another MN step and use the associated filter to discard triples

How to Invert a Round:



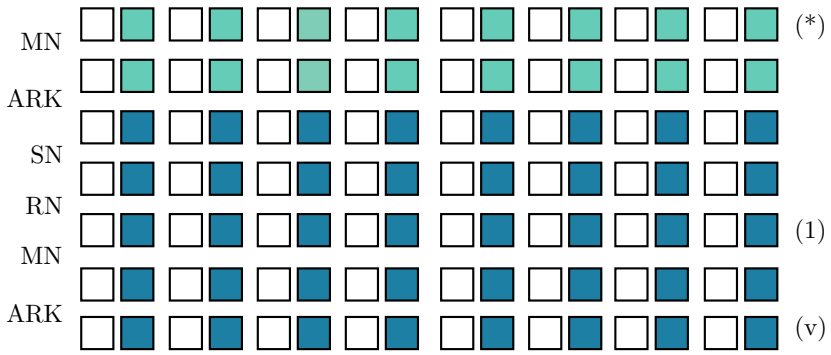
How to Invert a Round:



Given: Candidate triple that has passed the test at point (1)
Associated values of the state lower nibbles at point (v)

Goal: Compute the difference on the lower nibbles at point (*):

How to Invert a Round:

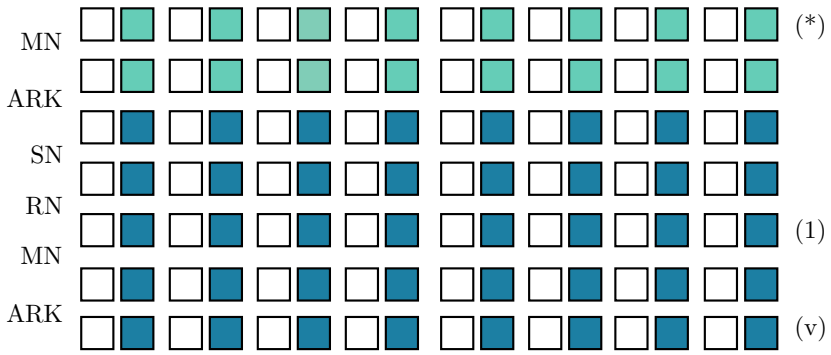


Given: Candidate triple that has passed the test at point (1)
Associated values of the state lower nibbles at point (v)

Goal: Compute the difference on the lower nibbles at point (*):

- Invert SN (value)

How to Invert a Round:

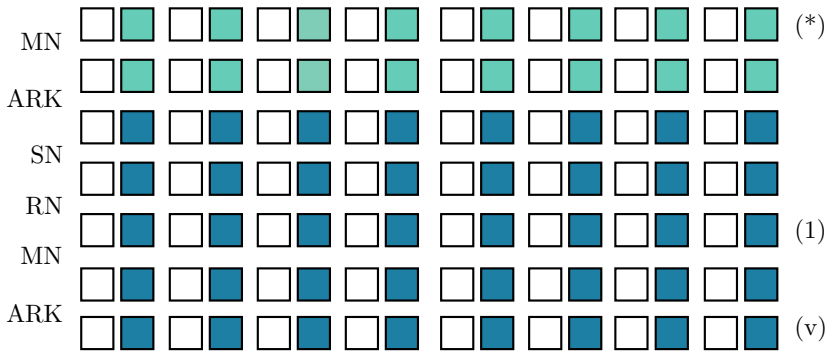


Given: Candidate triple that has passed the test at point (1)
Associated values of the state lower nibbles at point (v)

Goal: Compute the difference on the lower nibbles at point (*):

- Invert SN (value)
- Invert RN

How to Invert a Round:

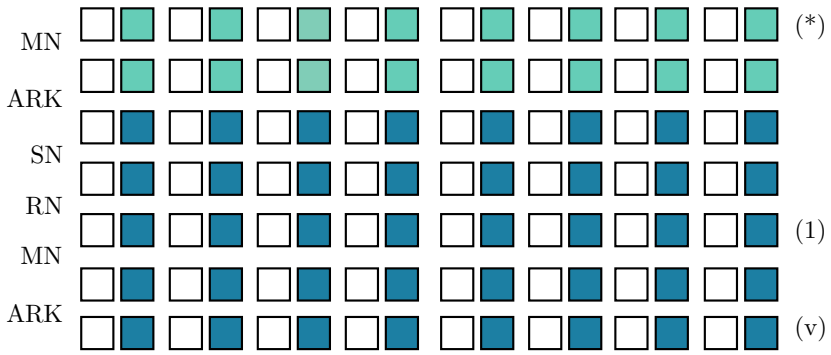


Given: Candidate triple that has passed the test at point (1)
Associated values of the state lower nibbles at point (v)

Goal: Compute the difference on the lower nibbles at point (*):

- Invert SN (value)
- Invert RN
- Invert ARK (Key Schedule property)

How to Invert a Round:



Given: Candidate triple that has passed the test at point (1)
Associated values of the state lower nibbles at point (v)

Goal: Compute the difference on the lower nibbles at point (*):

- Invert SN (value)
- Invert RN
- Invert ARK (Key Schedule property)
- We have to invert MN in lower nibbles

Inverting a Round: MN case

Let $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ be the binary decomposition of a byte a.
(a_0, a_1, a_2, a_3) the higher nibble
(a_4, a_5, a_6, a_7) the lower nibble

proposition

To compute the lower nibbles of the input of *MixColumn* given the lower nibbles of the output (a, b, c, d), we require 3 information bits from the higher nibbles:

$$\begin{cases} a_1 + a_2 + b_2 + c_0 + c_1 + c_2 + d_0 + d_2 \\ a_1 + b_0 + b_1 + c_1 + d_0 + d_1 \\ a_0 + a_1 + a_2 + b_0 + b_2 + c_1 + c_2 + d_2 \end{cases}$$

Inverting a Round: MN case

Let $(a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7)$ be the binary decomposition of a byte a.
(a_0, a_1, a_2, a_3) the higher nibble
(a_4, a_5, a_6, a_7) the lower nibble

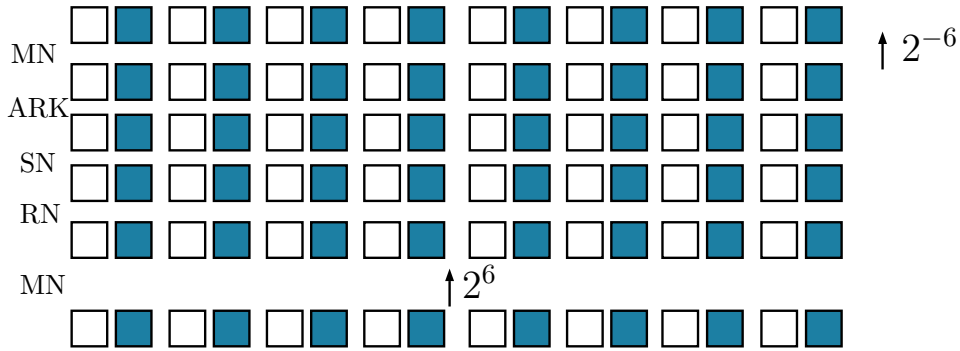
proposition

To compute the lower nibbles of the input of *MixColumn* given the lower nibbles of the output (a, b, c, d), we require 3 information bits from the higher nibbles:

$$\begin{cases} a_1 + a_2 + b_2 + c_0 + c_1 + c_2 + d_0 + d_2 \\ a_1 + b_0 + b_1 + c_1 + d_0 + d_1 \\ a_0 + a_1 + a_2 + b_0 + b_2 + c_1 + c_2 + d_2 \end{cases}$$

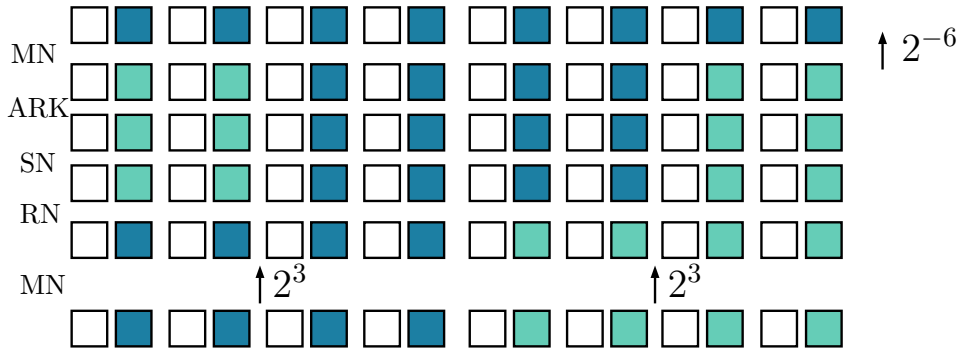
$\Rightarrow$ a 6-bit guess suffices to predict the lower nibbles entering MixNibble

Inverting a Round: MN case

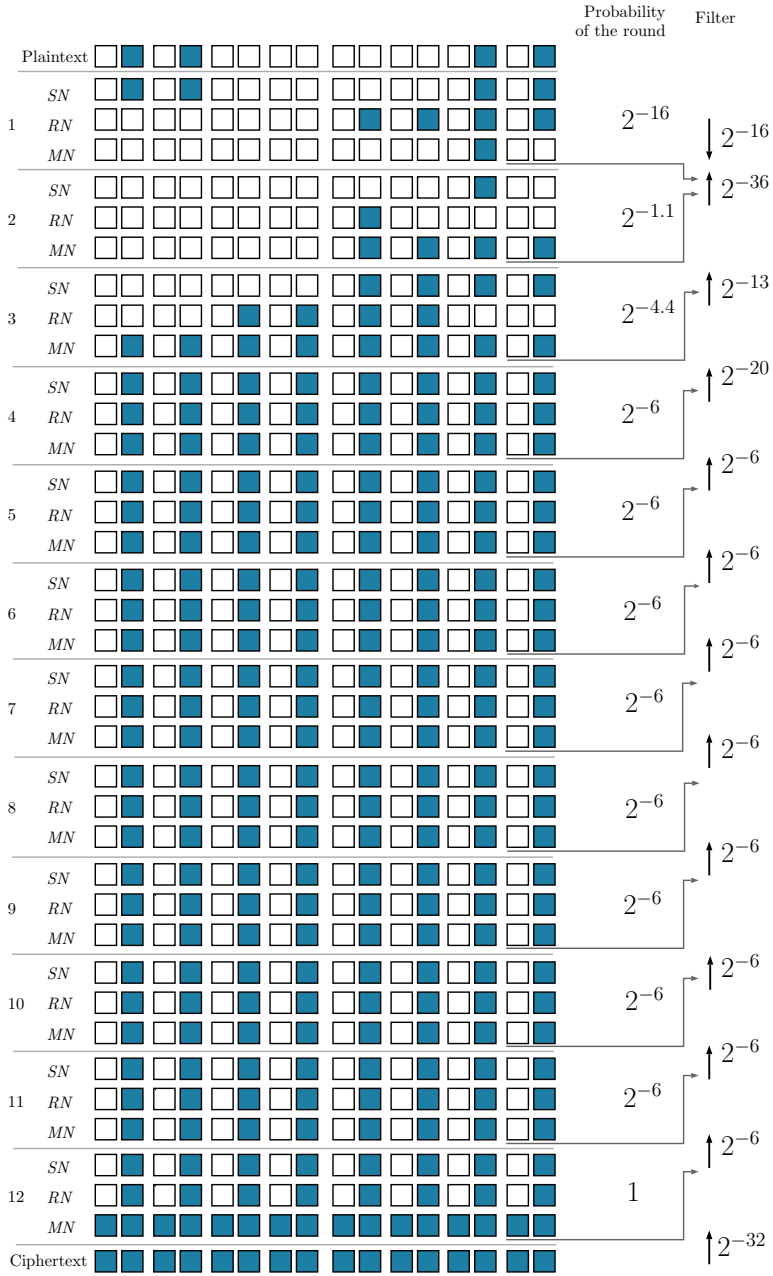


- We invert MN for the 2^6 possibilities for the 6-bit guesses
- The conditions on the previous MN give us a filter of 2^{-6}

Inverting a Round: MN case



- We invert MN for the 2^6 possibilities for the 6-bit guesses
- The conditions on the previous MN give us a filter of 2^{-6}
- We can invert independently the 2 MC to reduce the cost of this operation (2^4 round computations instead of 2^6)



Path of probability $2^{-69.5}$
For each pair with higher nibbles inactive before the last MN :

1. Guess the Lower Nibbles of the key and use the first round as a filter
2. Invert the last round with a 6-bit guess
3. Use the difference obtained before MN as a filter
4. Invert another round
5. The first rounds give us more efficient filters
6. Finally we compare the values of the lower nibbles recovered with the value of the plaintext

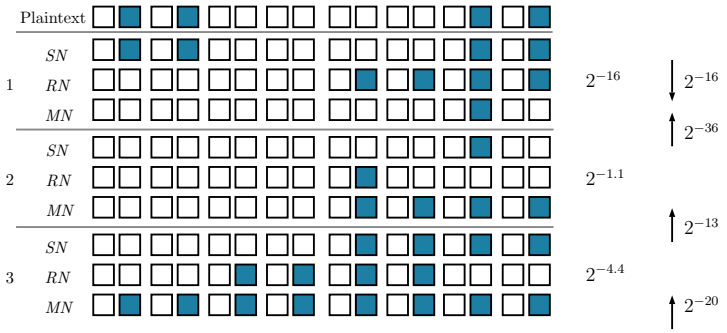
Results

- At the end, $2^{8.5}$ triples remain
- Higher Nibbles search discards the incorrect values

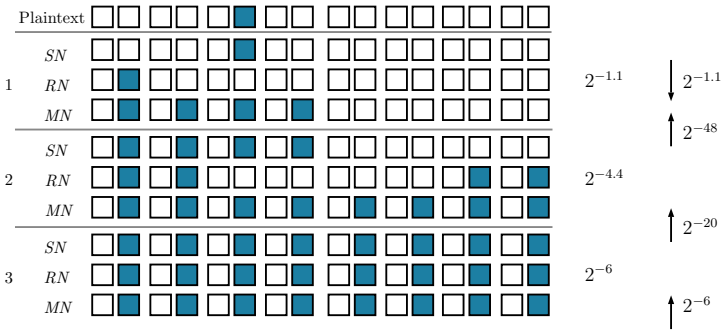
Source	Rounds	Data	Time	Memory	Attacks
[YWLZ 11]	7	$2^{34.3}$	$2^{45.5}$	2^{32}	integral
[YWLZ 11]	8	2^{32}	$2^{46.8}$	2^{16}	truncated
[ANS 11]	8	2^{35}	2^{35}	-	differential
[NWW 13]	10	1	2^{62}	2^{60}	PC MITM
[ASR 13]	12	2^{39}	$2^{62.84}$	$2^{4.5}$	biclique
Our New Attack	12	$2^{54.5}$	$2^{57.07}$	2^{16}	truncated

Trade-offs

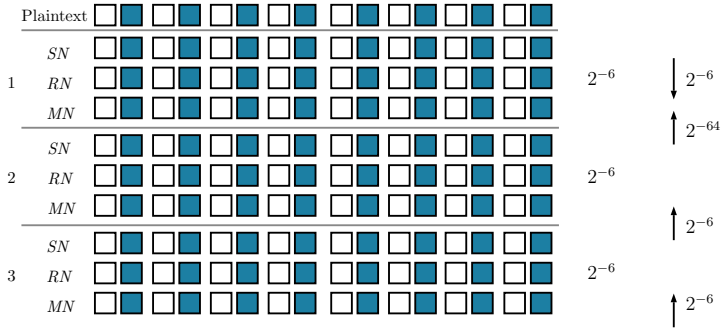
By changing the beginnings of the truncated differential paths, we obtain 4 interesting trade-offs:



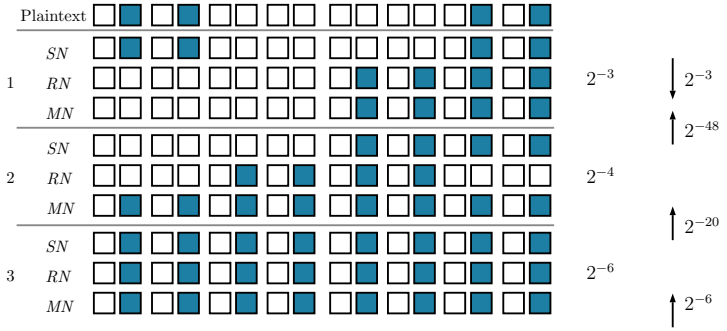
Case I



Case II



Case III



Case IV

Complexity of the Attacks on Full KLEIN-64

Resulting complexities for the 4 previous trade-offs

Case	Data	Time	Memory
1	$2^{54.5}$	2^{57}	2^{16}
2	$2^{56.5}$	2^{62}	2^{4}
3	2^{35}	$2^{63.8}$	2^{32}
4	2^{46}	2^{62}	2^{16}

Complexities for KLEIN-80 and KLEIN-96:

more rounds $\Rightarrow$ paths of lower probabilities
longer keys $\Rightarrow$ more lower nibbles to guess

Version	Case	Rounds	Data	Time	Memory
80	1	13	$2^{60.49}$	$2^{71.1}$	2^{16}
80	2	13	$2^{62.49}$	2^{76}	2^{4}
80	3	13	2^{41}	2^{78}	2^{32}
80	4	13	2^{52}	2^{76}	2^{16}
96	3	14	2^{47}	2^{92}	2^{32}
96	4	14	2^{58}	$2^{89.2}$	2^{16}

Complexities for KLEIN-80 and KLEIN-96:

more rounds $\Rightarrow$ paths of lower probabilities
longer keys $\Rightarrow$ more lower nibbles to guess

Version	Case	Rounds	Data	Time	Memory
80	1	13	$2^{60.49}$	$2^{71.1}$	2^{16}
80	2	13	$2^{62.49}$	2^{76}	2^{4}
80	3	13	2^{41}	2^{78}	2^{32}
80	4	13	2^{52}	2^{76}	2^{16}
96	3	14	2^{47}	2^{92}	2^{32}
96	4	14	2^{58}	$2^{89.2}$	2^{16}

We can attack

- 13 rounds out of 16 of KLEIN-80
- 14 rounds out of 20 of KLEIN-96

Conclusion

- First attack on the full version of KLEIN-64

Conclusion

- First attack on the full version of KLEIN-64
- Verified experimentally on round-reduced versions (first practical attacks on 10 rounds)

Conclusion

- First attack on the full version of KLEIN-64
- Verified experimentally on round-reduced versions (first practical attacks on 10 rounds)
- Changing the MDS matrix in MixNibble or the KeySchedule might counter these attacks

Thank you for your attention