New representations of the AES Key Schedule

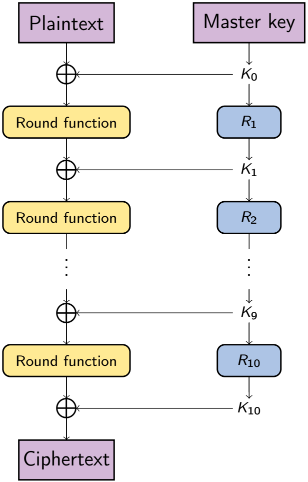
Gaëtan Leurent, Clara Pernot
Inria, Paris

AES: Advanced Encryption Standard [FIPS-197]

- The AES is the most widely used block cipher today.
- Winner of the AES competition.
- Subset of **Rijndael** block cipher.
- Designed by Rijmen and Daemen.
- **Block size**: 128 bits.
- **Key size**: 128, 192, 256 bits.

AES: Advanced Encryption Standard [FIPS-197]

- The AES is the most widely used block cipher today.
- Winner of the AES competition.
- Subset of **Rijndael** block cipher.
- Designed by Rijmen and Daemen.
- **Block size**: 128 bits.
- **Key size**: 128, 192, 256 bits.



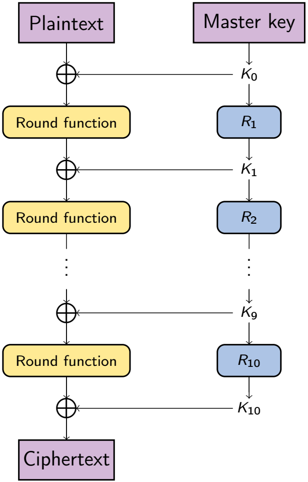
Description of the AES-128.

AES: Advanced Encryption Standard [FIPS-197]

- The AES is the most widely used block cipher today.
- Winner of the AES competition.
- Subset of **Rijndael** block cipher.
- Designed by Rijmen and Daemen.
- **Block size**: 128 bits.
- **Key size**: 128, 192, 256 bits.

After 20 years of cryptanalysis:

- only **7 rounds out of 10** are broken.
- the **key schedule** is known to **cause issues** in the related-key setting.



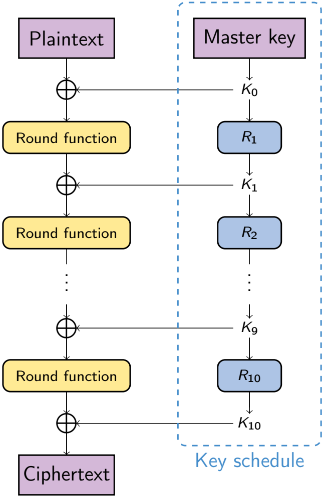
Description of the AES-128.

AES: Advanced Encryption Standard [FIPS-197]

- The AES is the most widely used block cipher today.
- Winner of the AES competition.
- Subset of **Rijndael** block cipher.
- Designed by Rijmen and Daemen.
- **Block size**: 128 bits.
- **Key size**: 128, 192, 256 bits.

After 20 years of cryptanalysis:

- only **7 rounds out of 10** are broken.
- the **key schedule** is known to **cause issues** in the related-key setting.



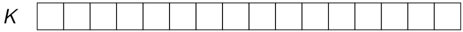
Description of the AES-128.

AES Key Schedule

The AES key schedule is used to derive **11 subkeys** from a master key K.

AES Key Schedule

The AES key schedule is used to derive **11 subkeys** from a master key K.

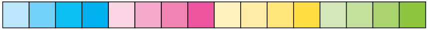


Division of the key into words and representation of the words in a matrix.

AES Key Schedule

The AES key schedule is used to derive **11 subkeys** from a master key K.

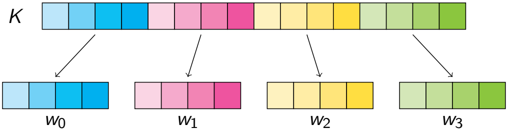
K



Division of the key into words and representation of the words in a matrix.

AES Key Schedule

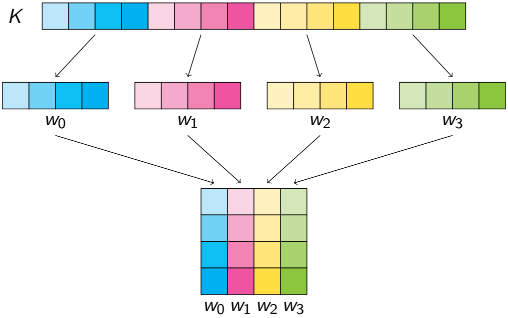
The AES key schedule is used to derive **11 subkeys** from a master key K.



Division of the key into words and representation of the words in a matrix.

AES Key Schedule

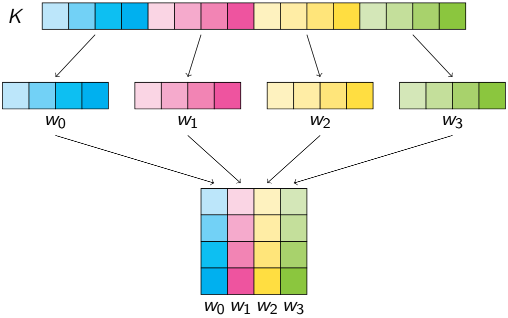
The AES key schedule is used to derive **11 subkeys** from a master key K.



Division of the key into words and representation of the words in a matrix.

AES Key Schedule

The AES key schedule is used to derive **11 subkeys** from a master key K.

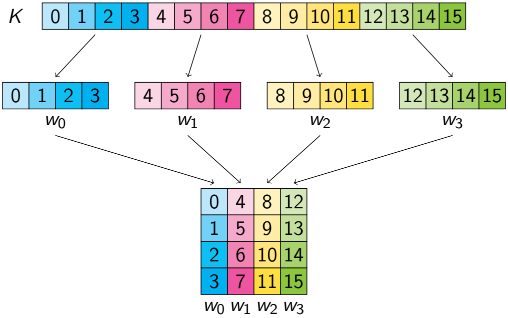


Division of the key into words and representation of the words in a matrix.

$\rightarrow$ The subkey at round i is the concatenation of the words $\mathrm{w}_{4\mathrm{i}}$ to $\mathrm{w}_{3+4\mathrm{i}}$.

AES Key Schedule

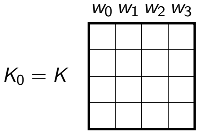
The AES key schedule is used to derive **11 subkeys** from a master key K.



Division of the key into words and representation of the words in a matrix.

$\rightarrow$ The subkey at round i is the concatenation of the words $\mathrm{w}_{4\mathrm{i}}$ to $\mathrm{w}_{3+4\mathrm{i}}$.

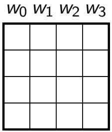
AES Key Schedule



Construction of words w_i for $i \geq 4$.

AES Key Schedule

$K_0 = K$



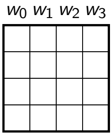
K_1

Construction of words w_i for $i \geq 4$.

AES Key Schedule

The leftmost column:

$K_0 = K$



K_1

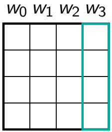
$$\mathsf{w_i} = \mathsf{SubWord}(\mathsf{RotWord}(\mathsf{w_{i-1}})) \oplus \mathsf{RCon}(i/4) \oplus \mathsf{w_{i-4}}$$

Construction of words $\mathsf{w_i}$ for $i \geq 4$.

AES Key Schedule

The leftmost column:

$K_0 = K$



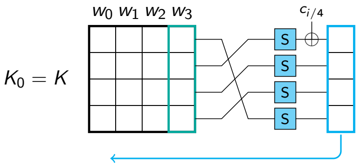
K_1

$$\mathsf{w_i} = \mathsf{SubWord}(\mathsf{RotWord}(\mathsf{w_{i-1}})) \oplus \mathsf{RCon}(i/4) \oplus \mathsf{w_{i-4}}$$

Construction of words $\mathsf{w_i}$ for $i \geq 4$.

AES Key Schedule

The leftmost column:



K_1

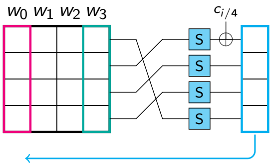
$w_i = \text{SubWord}(\text{RotWord}(w_{i-1})) \oplus \text{RCon}(i/4) \oplus w_{i-4}$

Construction of words w_i for $i \geq 4$.

AES Key Schedule

The leftmost column:

$K_0 = K$



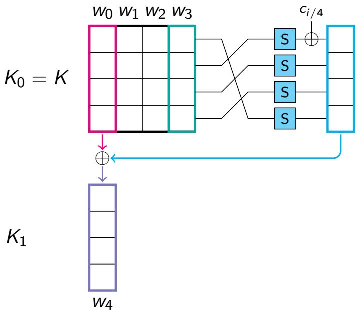
K_1

$\mathrm{w_i} = \mathrm{SubWord}(\mathrm{RotWord}(\mathrm{w_{i-1}})) \oplus \mathrm{RCon}(i/4) \oplus \mathrm{w_{i-4}}$

Construction of words $\mathrm{w_i}$ for $i \geq 4$.

AES Key Schedule

The leftmost column:

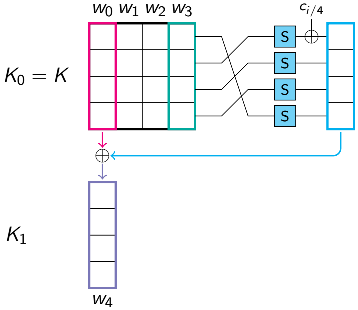


$\mathrm{w_i} = \mathrm{SubWord}(\mathrm{RotWord}(\mathrm{w_{i-1}})) \oplus \mathrm{RCon}(i/4) \oplus \mathrm{w_{i-4}}$

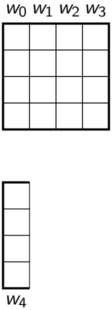
Construction of words $\mathrm{w_i}$ for $i \geq 4$.

AES Key Schedule

The leftmost column:

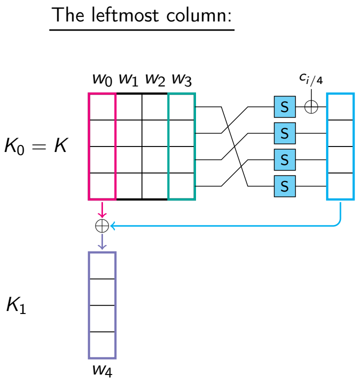


$\mathrm{w_i} = \mathrm{SubWord}(\mathrm{RotWord}(\mathrm{w_{i-1}})) \oplus \mathrm{RCon}(i/4) \oplus \mathrm{w_{i-4}}$

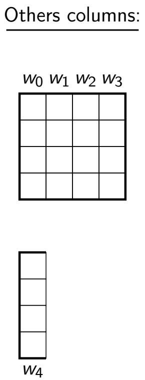


Construction of words $\mathrm{w_i}$ for $i \geq 4$.

AES Key Schedule



$\mathrm{w_i} = \mathrm{SubWord}(\mathrm{RotWord}(\mathrm{w_{i-1}})) \oplus \mathrm{RCon}(i/4) \oplus \mathrm{w_{i-4}}$

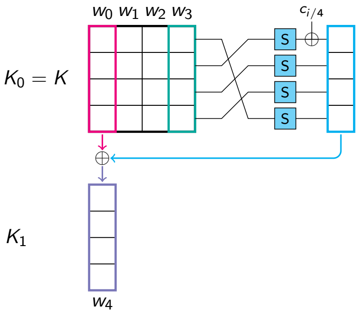


$\mathrm{w_i} = \mathrm{w_{i-1}} \oplus \mathrm{w_{i-4}}$

Construction of words $\mathrm{w_i}$ for $i \geq 4$.

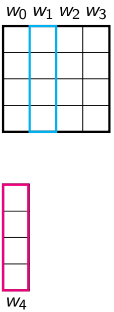
AES Key Schedule

The leftmost column:



$$\mathrm{w_i} = \mathrm{SubWord}(\mathrm{RotWord}(\mathrm{w_{i-1}})) \oplus \mathrm{RCon}(i/4) \oplus \mathrm{w_{i-4}}$$

Others columns:

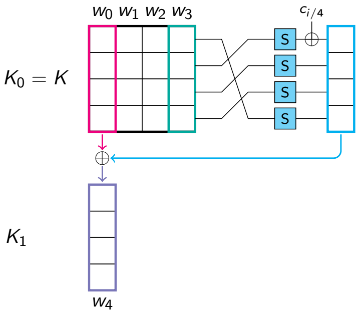


$$\mathrm{w_i} = \mathrm{w_{i-1}} \oplus \mathrm{w_{i-4}}$$

Construction of words $\mathrm{w_i}$ for $i \geq 4$.

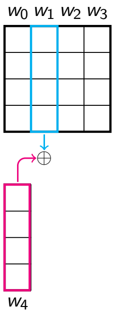
AES Key Schedule

The leftmost column:



$$\mathrm{w_i} = \mathrm{SubWord}(\mathrm{RotWord}(\mathrm{w_{i-1}})) \oplus \mathrm{RCon}(i/4) \oplus \mathrm{w_{i-4}}$$

Others columns:

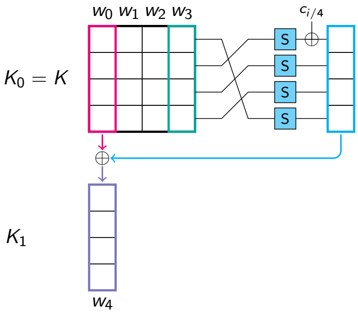


$$\mathrm{w_i} = \mathrm{w_{i-1}} \oplus \mathrm{w_{i-4}}$$

Construction of words $\mathrm{w_i}$ for $i \geq 4$.

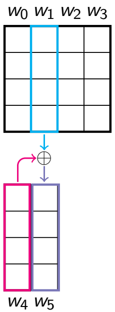
AES Key Schedule

The leftmost column:



$\mathrm{w_i} = \mathrm{SubWord}(\mathrm{RotWord}(\mathrm{w_{i-1}})) \oplus \mathrm{RCon}(i/4) \oplus \mathrm{w_{i-4}}$

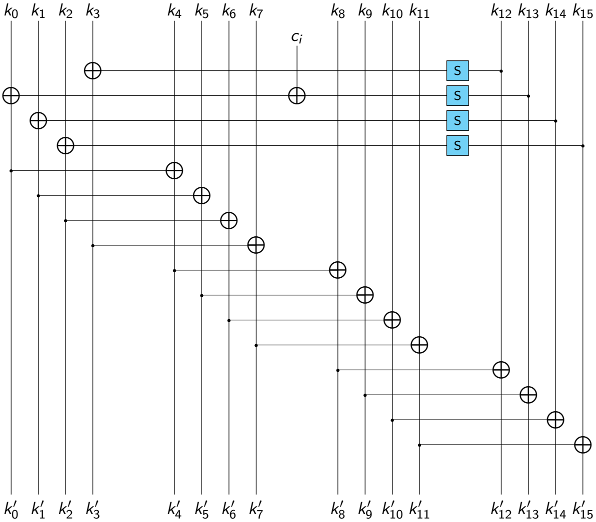
Others columns:



$\mathrm{w_i} = \mathrm{w_{i-1}} \oplus \mathrm{w_{i-4}}$

Construction of words $\mathrm{w_i}$ for $i \geq 4$.

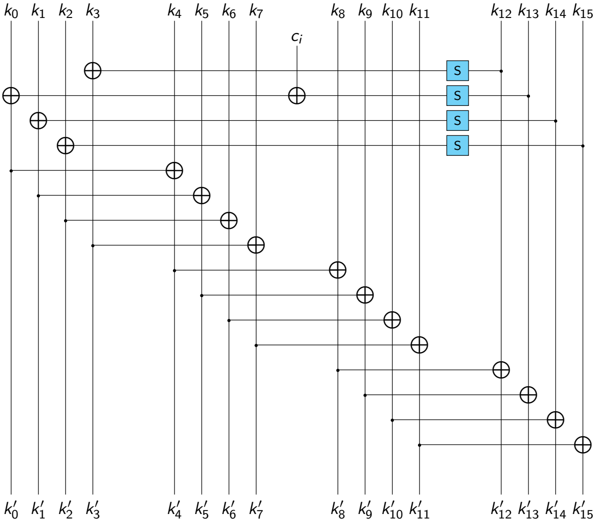
AES key schedule



One round of the AES key schedule.

AES key schedule

Impression: all bytes are mixed!



One round of the AES key schedule.

Our results

- **Alternative representations** of the AES key schedules

> **Even after a large number of rounds,**
> **the key schedule does not mix all the bytes!**

Our results

- **Alternative representations** of the AES key schedules

**Even after a large number of rounds,
the key schedule does not mix all the bytes!**

- **Short length cycles** when iterating an odd number of rounds of key schedule
  - Attacks on **mixFeed** and **ALE**

Our results

- **Alternative representations** of the AES key schedules

  Even after a large number of rounds,
  the key schedule does not mix all the bytes!

- **Short length cycles** when iterating an odd number of rounds of key schedule
  - Attacks on **mixFeed** and **ALE**

- **Efficient combination of information** from subkeys
  - Improvement of **Impossible Differential** and **Square** attacks against the AES

Table of contents

Difference diffusion

Invariant subspaces: a subspace A and an offset u such as:

$$\boxed{\exists\ u,\ \ F(A+u) = A + F(u)}$$

Difference diffusion

Invariant subspaces: a subspace A and an offset u such as:

$$\boxed{\exists\, u,\;\; F(A+u) = A + F(u)}$$

Subspace trails: a subspace A and an offset u such as:

$$\boxed{\forall\, u,\;\; F(A+u) = B + F(u)}$$

Difference diffusion

Invariant subspaces: a subspace A and an offset u such as:

$$\boxed{\exists\, u,\ \ F(A+u) = A + F(u)}$$

Subspace trails: a subspace A and an offset u such as:

$$\boxed{\forall\, u,\ \ F(A+u) = B + F(u)}$$

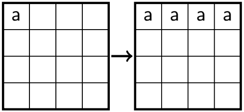
$\Rightarrow$ [LMR, EC'15] introduced an algorithm to **detect invariant subspaces**

Difference diffusion

a			

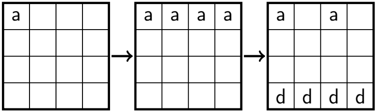
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



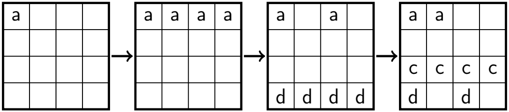
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



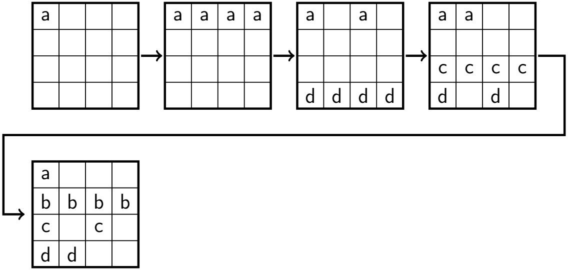
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



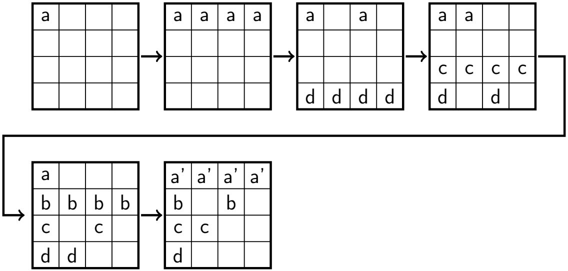
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



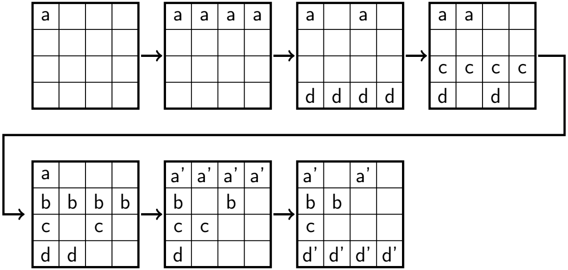
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



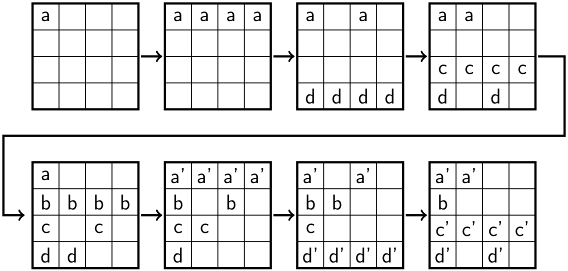
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



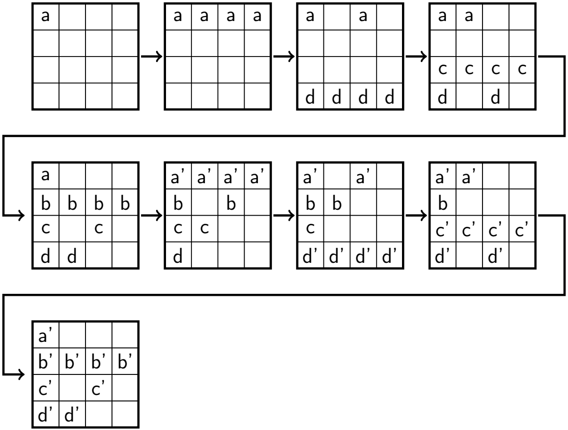
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



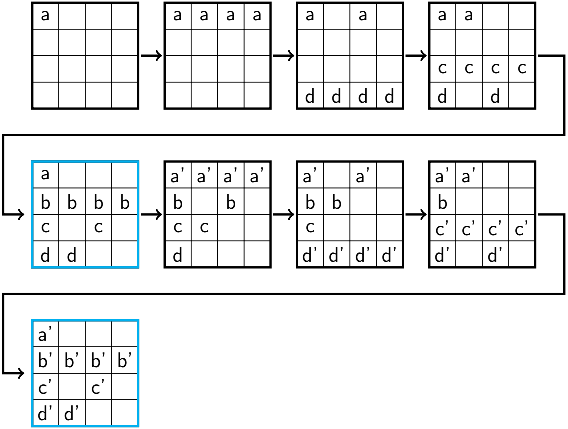
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



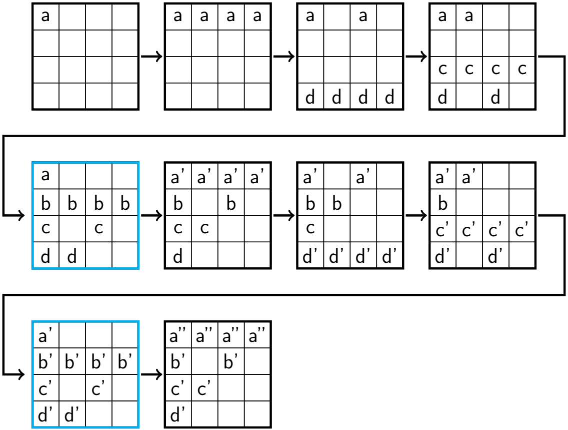
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



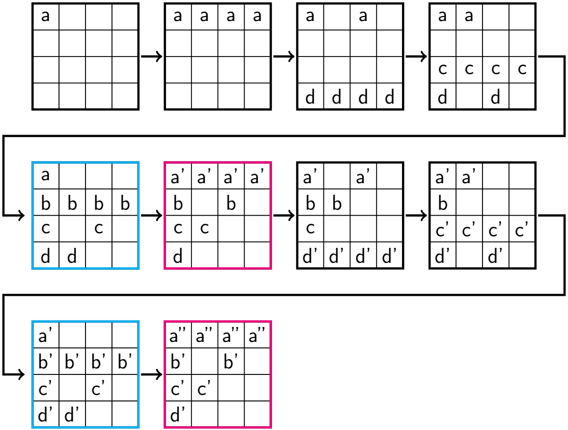
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



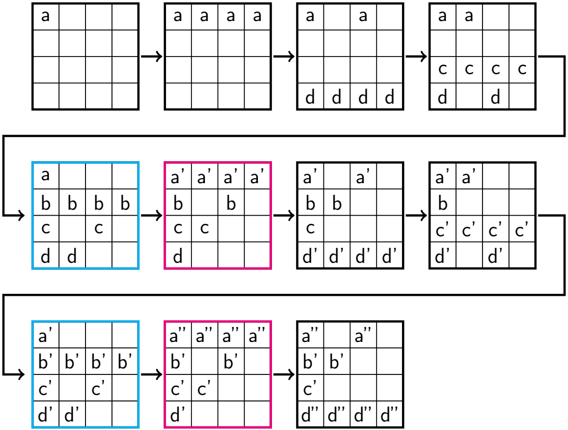
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



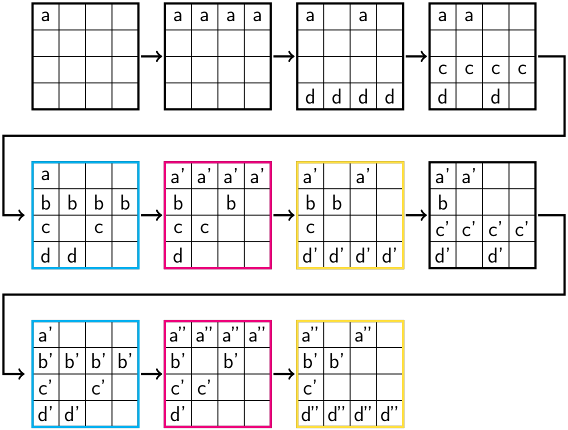
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



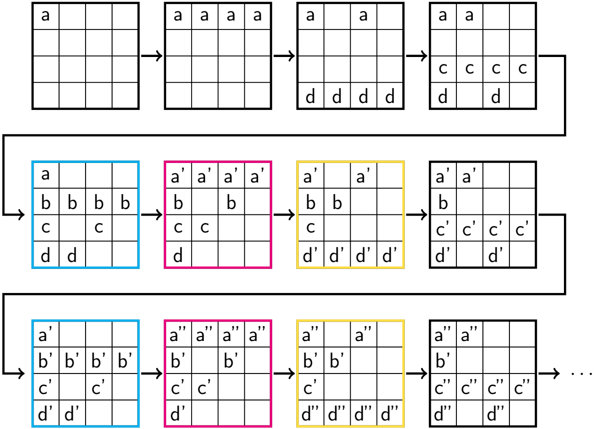
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



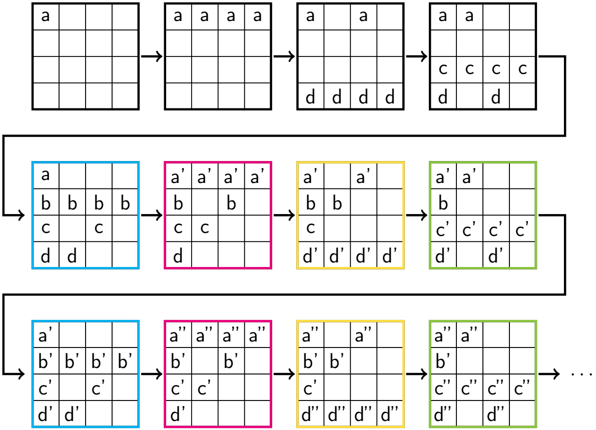
Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion



Diffusion of a difference on the first byte after several rounds of key schedule.

Difference diffusion

We obtain **4 families of subspace trails** whose linear parts are:

- $E_0 = \{(a, b, c, d, 0, b, 0, d, a, 0, 0, d, 0, 0, 0, d)$ with $a, b, c, d \in \mathbb{F}_{2^8}\}$
- $E_1 = \{(a, b, c, d, a, 0, c, 0, 0, 0, c, d, 0, 0, c, 0)$ with $a, b, c, d \in \mathbb{F}_{2^8}\}$
- $E_2 = \{(a, b, c, d, 0, b, 0, d, 0, b, c, 0, 0, b, 0, 0)$ with $a, b, c, d \in \mathbb{F}_{2^8}\}$
- $E_3 = \{(a, b, c, d, a, 0, c, 0, a, b, 0, 0, a, 0, 0, 0)$ with $a, b, c, d \in \mathbb{F}_{2^8}\}$

$$\boxed{\forall u \in (\mathbb{F}_{2^8})^{16}, R(E_i + u) = E_{i+1} + R(u)}$$

The full space is the direct sum of those four vector spaces:

$$(\mathbb{F}_{2^8})^{16} = E_0 \oplus E_1 \oplus E_2 \oplus E_3$$

New representation of the AES Key Schedule

We perform a **linear transformation** $A = C_0^{-1}$, which corresponds to a change of basis:

Basis of E_0:

$$s_0 = k_{15} \quad s_1 = k_{14} \oplus k_{10} \oplus k_6 \oplus k_2 \quad s_2 = k_{13} \oplus k_5 \quad s_3 = k_{12} \oplus k_8$$

Basis of E_1:

$$s_4 = k_{14} \quad s_5 = k_{13} \oplus k_9 \oplus k_5 \oplus k_1 \quad s_6 = k_{12} \oplus k_4 \quad s_7 = k_{15} \oplus k_{11}$$

Basis of E_2:

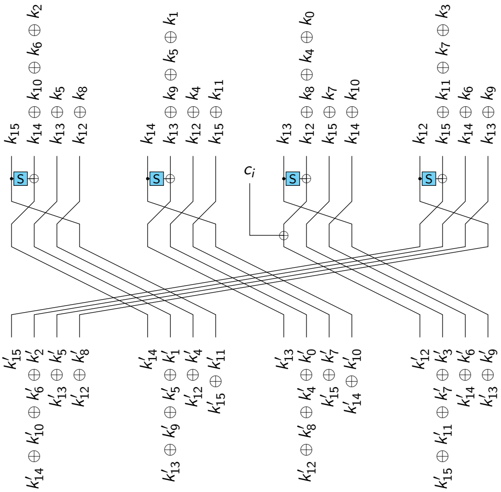
$$s_8 = k_{13} \quad s_9 = k_{12} \oplus k_8 \oplus k_4 \oplus k_0 \quad s_{10} = k_{15} \oplus k_7 \quad s_{11} = k_{14} \oplus k_{10}$$

Basis of E_3:

$$s_{12} = k_{12} \quad s_{13} = k_{15} \oplus k_{11} \oplus k_7 \oplus k_3 \quad s_{14} = k_{14} \oplus k_6 \quad s_{15} = k_{13} \oplus k_9$$

$\Rightarrow$ The **4 subspaces** appear more clearly!

New representation of the AES Key Schedule

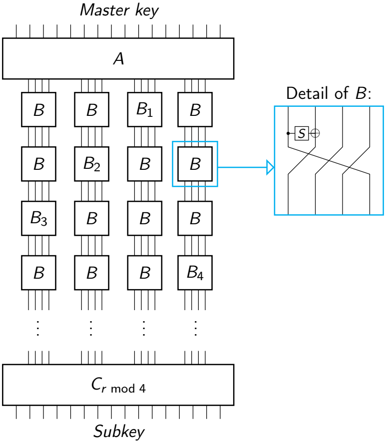


One round of the AES key schedule (alternative representation).

- 4 subspace trails
- 4 independent functions

The key schedule does not mix all the bytes!

New representation of the AES Key Schedule



r rounds of the key schedule in the new representation.

- B_i is similar to B but the round constant c_i is XORed to the output of the S-box.
- $C_i = A^{-1} \times \mathrm{SR}^i$, with SR the matrix corresponding to rotation of 4 bytes to the right.

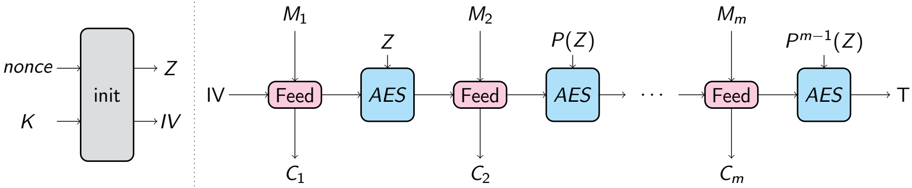
Table of contents

Table of contents

mixFeed [Chakraborty and Nandi, NIST LW Submission]

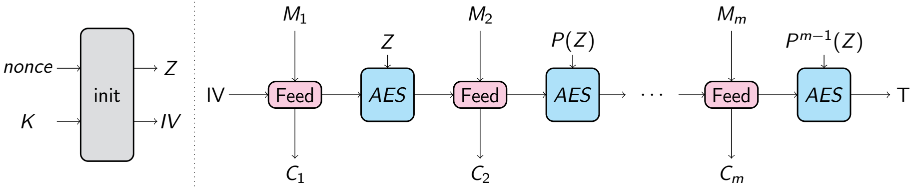
- mixFeed was a **second-round candidate** in the NIST Lightweight Standardization Process which was **not selected as a finalist**
- Submitted by Bishwajit **Chakraborty** and Mridul **Nandi**
- **AEAD** (Authenticated Encryption with Associated Data) algorithm
- Based on the AES block cipher

mixFeed

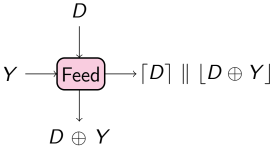


Simplified scheme of mixFeed encryption.

mixFeed

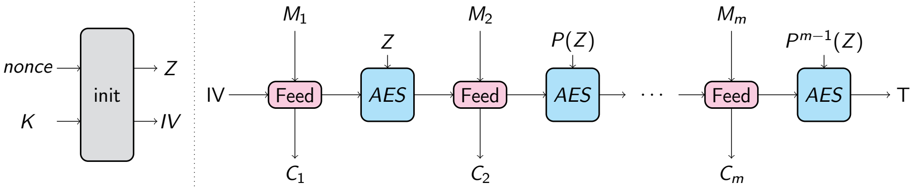


Simplified scheme of mixFeed encryption.

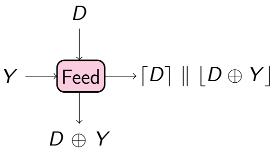


Function Feed in the case where
$|D| = 128$

mixFeed



Simplified scheme of mixFeed encryption.



Function Feed in the case where $|D| = 128$

P: **11 rounds** of key schedule

P is **iterated** $\rightarrow$ we study its **cycles**!

Mustafa Khairallah's observation [ToSC'19]

000102030405060708090a0b0c0d0e0f
00020406080a0c0e10121416181a1c1e
0004080c1014181c2024282c3034383c
00081018202830384048505860687078
00102030405060708090a0b0c0d0e0f0
101112131415161718191a1b1c1d1e1f
20222426282a2c2e30323436383a3c3e
4044484c5054585c6064686c7074787c
80889098a0a8b0b8c0c8d0d8e0e8f0f8
303132333435363738393a3b3c3d3e3f
707172737475767778797a7b7c7d7e7f
000306090c0f1215181b1e2124272a2d
00050a0f14191e23282d32373c41464b
00070e151c232a31383f464d545b6269
000d1a2734414e5b6875828f9ca9b6c3
00152a3f54697e93a8bdd2e7fc11263b
00172e455c738aa1b8cfe6fd142b4259
00183048607890a8c0d8f00820385068
001c3854708ca8c4e0fc1834506c88a4
001f3e5d7c9bbad9f81736557493b2d1

Using brute-force and out of 33 tests, Khairallah found **20 cycles of length**

$$\mathbf{14018661024} \approx 2^{33.7}$$

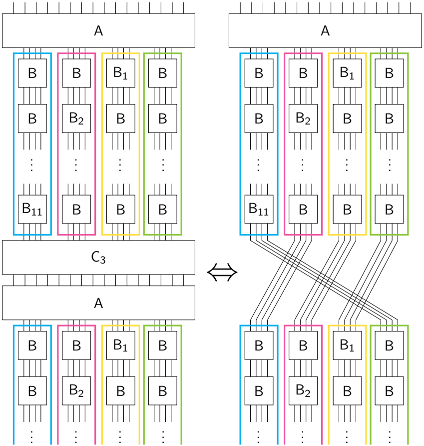
for the P permutation.

Surprising facts:

- $\rightarrow$ all cycles found are of the same length
- $\rightarrow$ this length is much smaller than the cycle length expected for a 128-bit permutation

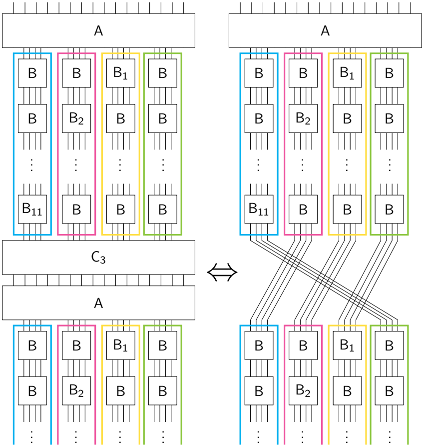
Table of contents

Cycle analysis of 11-round AES key schedule



Two iterations of 11 rounds of the key schedule in the new representation.

Cycle analysis of 11-round AES key schedule



Two iterations of 11 rounds of the key schedule in the new representation.

We define:

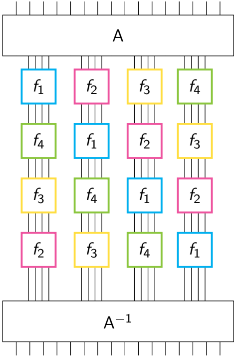
$$\boxed{f_1} = B_{11} \circ B \circ B \circ B \circ B_7 \circ B \circ B \circ B \circ B_3 \circ B \circ B$$

$$\boxed{f_2} = B \circ B_{10} \circ B \circ B \circ B \circ B_6 \circ B \circ B \circ B \circ B_2 \circ B$$

$$\boxed{f_3} = B \circ B \circ B_9 \circ B \circ B \circ B \circ B_5 \circ B \circ B \circ B \circ B_1$$

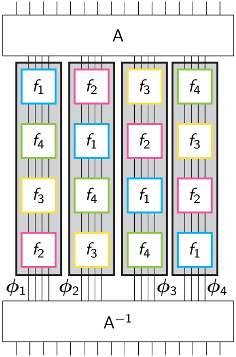
$$\boxed{f_4} = B \circ B \circ B \circ B_8 \circ B \circ B \circ B \circ B_4 \circ B \circ B \circ B$$

Cycle analysis of 11-round AES key schedule

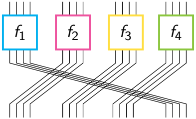


4 iterations of P in the new model.

Cycle analysis of 11-round AES key schedule



4 iterations of P in the new model.



$$\widetilde{P} = A \circ P \circ A^{-1}$$

$$\widetilde{P} : (a, b, c, d) \mapsto (f_2(b), f_3(c), f_4(d), f_1(a))$$

$$\widetilde{P}^4 : (a, b, c, d) \mapsto (\phi_1(a), \phi_2(b), \phi_3(c), \phi_4(d))$$

$$\phi_1(a) = f_2 \circ f_3 \circ f_4 \circ f_1(a)$$

$$\phi_2(b) = f_3 \circ f_4 \circ f_1 \circ f_2(b)$$

$$\phi_3(c) = f_4 \circ f_1 \circ f_2 \circ f_3(c)$$

$$\phi_4(d) = f_1 \circ f_2 \circ f_3 \circ f_4(d)$$

Cycle analysis of 11-round AES key schedule

- If (a, b, c, d) is in a cycle of length ℓ of $\widetilde{P}^4$, we have:

$$\phi_1^\ell(a) = a \qquad \phi_2^\ell(b) = b \qquad \phi_3^\ell(c) = c \qquad \phi_4^\ell(d) = d$$

  In particular, a, b, c and d must be in cycles of ϕ_1, ϕ_2, ϕ_3, ϕ_4 (respectively) of **length dividing ℓ**.

Cycle analysis of 11-round AES key schedule

- If (a, b, c, d) is in a cycle of length ℓ of $\widetilde{P}^4$, we have:

  $$\phi_1^\ell(a) = a \qquad \phi_2^\ell(b) = b \qquad \phi_3^\ell(c) = c \qquad \phi_4^\ell(d) = d$$

  In particular, a, b, c and d must be in cycles of ϕ_1, ϕ_2, ϕ_3, ϕ_4 (respectively) of **length dividing ℓ**.

- Conversely, if a, b, c, d are in cycles of the corresponding ϕ_i, then (a, b, c, d) is in a cycle of $\widetilde{P}^4$ of length the **lowest common multiple of the small cycle lengths**.

Cycle analysis of 11-round AES key schedule

- If (a, b, c, d) is in a cycle of length ℓ of $\widetilde{P}^4$, we have:

$$\phi_1^\ell(a) = a \qquad \phi_2^\ell(b) = b \qquad \phi_3^\ell(c) = c \qquad \phi_4^\ell(d) = d$$

  In particular, a, b, c and d must be in cycles of ϕ_1, ϕ_2, ϕ_3, ϕ_4 (respectively) of **length dividing ℓ**.

- Conversely, if a, b, c, d are in cycles of the corresponding ϕ_i, then (a, b, c, d) is in a cycle of $\widetilde{P}^4$ of length the **lowest common multiple of the small cycle lengths**.

- Due to the structure of the ϕ_i functions, all of them have the **same cycle structure**:

$$\phi_2 = f_2^{-1} \circ \phi_1 \circ f_2; \qquad \phi_3 = f_3^{-1} \circ \phi_2 \circ f_3; \qquad \phi_4 = f_4^{-1} \circ \phi_3 \circ f_4$$

Cycle analysis of 11-round AES key schedule

Length	# cycles	Proba	Smallest element
3504665256	1	0.82	00 00 00 01
255703222	1	0.05	00 00 00 0b
219107352	1	0.05	00 00 00 1d
174977807	1	0.04	00 00 00 00
99678312	1	0.02	00 00 00 21
13792740	1	0.003	00 00 00 75
8820469	1	$2^{-8,93}$	00 00 00 24
7619847	1	$2^{-9,14}$	00 00 00 c1
5442633	1	$2^{-9,63}$	00 00 02 78
4214934	1	2^{-10}	00 00 05 77
459548	1	$2^{-13,2}$	00 00 38 fe
444656	1	$2^{-13,24}$	00 00 0b 68
14977	1	$2^{-18,13}$	00 06 82 5c
14559	1	$2^{-18,18}$	00 04 fa b1
5165	1	$2^{-19,67}$	00 0a d4 4e
4347	1	$2^{-19,92}$	00 04 94 3a
1091	1	$2^{-21.91}$	00 21 4b 3b
317	1	$2^{-23,7}$	00 28 41 36
27	1	$2^{-27,25}$	01 3a 0d 0c
6	1	$2^{-29,42}$	06 23 25 51
5	3	$3 \cdot 2^{-29,68}$	06 1a ea 18
4	2	$2 \cdot 2^{-30}$	23 c6 6f 2b
2	3	$3 \cdot 2^{-31}$	69 ea 63 75
1	2	$2 \cdot 2^{-32}$	7e be d1 92

Cycle structure of ϕ_1 for 11-round AES-128 key schedule.

Cycle analysis of 11-round AES key schedule

Length	# cycles	Proba	Smallest element
$\boxed{3504665256}$	1	$\boxed{0.82}$	`00 00 00 01`
255703222	1	0.05	`00 00 00 0b`
219107352	1	0.05	`00 00 00 1d`
174977807	1	0.04	`00 00 00 00`
99678312	1	0.02	`00 00 00 21`
13792740	1	0.003	`00 00 00 75`
8820469	1	$2^{-8,93}$	`00 00 00 24`
7619847	1	$2^{-9,14}$	`00 00 00 c1`
5442633	1	$2^{-9,63}$	`00 00 02 78`
4214934	1	2^{-10}	`00 00 05 77`
459548	1	$2^{-13,2}$	`00 00 38 fe`
444656	1	$2^{-13,24}$	`00 00 0b 68`
14977	1	$2^{-18,13}$	`00 06 82 5c`
14559	1	$2^{-18,18}$	`00 04 fa b1`
5165	1	$2^{-19,67}$	`00 0a d4 4e`
4347	1	$2^{-19,92}$	`00 04 94 3a`
1091	1	$2^{-21.91}$	`00 21 4b 3b`
317	1	$2^{-23,7}$	`00 28 41 36`
27	1	$2^{-27,25}$	`01 3a 0d 0c`
6	1	$2^{-29,42}$	`06 23 25 51`
5	3	$3 \cdot 2^{-29,68}$	`06 1a ea 18`
4	2	$2 \cdot 2^{-30}$	`23 c6 6f 2b`
2	3	$3 \cdot 2^{-31}$	`69 ea 63 75`
1	2	$2 \cdot 2^{-32}$	`7e be d1 92`

Cycle structure of ϕ_1 for 11-round AES-128 key schedule.

With probability $0.82^4 \simeq 0.45$, we have a, b, c and d in a cycle of length $\ell = 3504665256$, resulting in:

- $\rightarrow$ a cycle of length ℓ for $\widetilde{P}^4$,
- $\rightarrow$ a cycle of length at most $4\ell = 14018661024$ for $\widetilde{P}$ and P.

Cycle analysis of 11-round AES key schedule

Summary: 45% of keys belong to cycles of length 14018661024 $\approx 2^{33.7}$.

Cycle analysis of 11-round AES key schedule

Summary: 45% of keys belong to cycles of length 14018661024 $\approx 2^{33.7}$.

→ This explains the observation on mixFeed [Khairallah, ToSC'19].

→ This allows to make a forgery against mixFeed.

Cycle analysis of 11-round AES key schedule

Summary: 45% of keys belong to cycles of length 14018661024 $\approx 2^{33.7}$.

→ This explains the observation on mixFeed [Khairallah, ToSC'19].

→ This allows to make a forgery against mixFeed.

→ This contradicts the assumption made in a security proof of mixFeed:

Assumption [Chakraborty and Nandi, NIST LW Workshop]

For any $K \in \{0,1\}^n$ chosen uniformly at random, probability that K has a period at most ℓ is at most $\ell/2^{n/2}$.

Table of contents

Forgery attack against mixFeed [Khairallah, ToSC'19]

The goal of a **forgery attack** is to forge a valid tag T'
for a new ciphertext C' using (M, C, T).

Forgery attack against mixFeed [Khairallah, ToSC'19]

The goal of a **forgery attack** is to forge a valid tag T' for a new ciphertext C' using (M, C, T).

Khairallah proposed a forgery attack against mixFeed:

- we assume that Z belongs to a **cycle** of length ℓ
- we choose a message M made of m blocks, with $m > \ell$

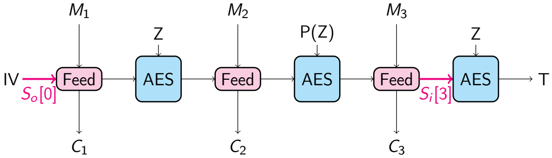
Forgery attack against mixFeed [Khairallah, ToSC'19]

The goal of a **forgery attack** is to forge a valid tag T' for a new ciphertext C' using (M, C, T).

Khairallah proposed a forgery attack against mixFeed:

- we assume that Z belongs to a **cycle** of length ℓ
- we choose a message M made of m blocks, with $m > \ell$

(1) Cut



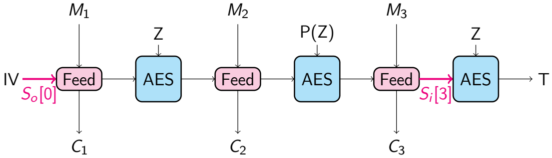
Forgery attack against mixFeed [Khairallah, ToSC'19]

The goal of a **forgery attack** is to forge a valid tag T' for a new ciphertext C' using (M, C, T).

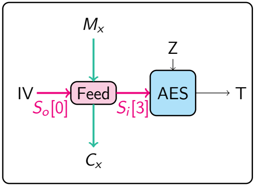
Khairallah proposed a forgery attack against mixFeed:

- we assume that Z belongs to a **cycle** of length ℓ
- we choose a message M made of m blocks, with $m > \ell$

(1) Cut



(2) Paste



Forgery attack against mixFeed

Summary of the forgery attack:

→ Data complexity: a known plaintext of length higher than $2^{37.7}$ bytes

→ Memory complexity: negligible

→ Time complexity: negligible

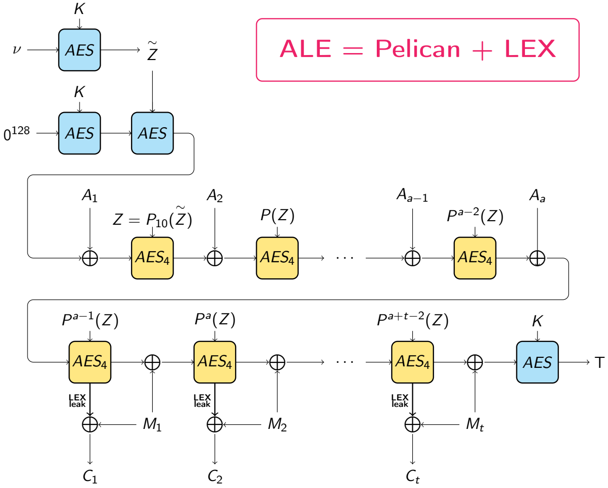
→ Success rate: 45%

⇒ Verified using the mixFeed reference implementation:

41 successes out of 100 tests!

Table of contents

Application to ALE [**FSE:BMRRT13**]



Authenticated encryption with ALE.

→ Each AES encryption is expected to be performed with different keys.

Application to ALE

$\rightarrow$ Using the same approach as for mixFeed: 76% of the keys belong to cycles of length 16043203220 $\approx 2^{33.9}$.

$\rightarrow$ Short length cycles allows to find states encrypted under the same key.

$\rightarrow$ New attacks are found using [BDF, Crypto'11].

Application to ALE

→ Using the same approach as for mixFeed: 76% of the keys belong to cycles of length 16043203220 $\approx 2^{33.9}$.

→ Short length cycles allows to find states encrypted under the same key.

→ New attacks are found using [BDF, Crypto'11].

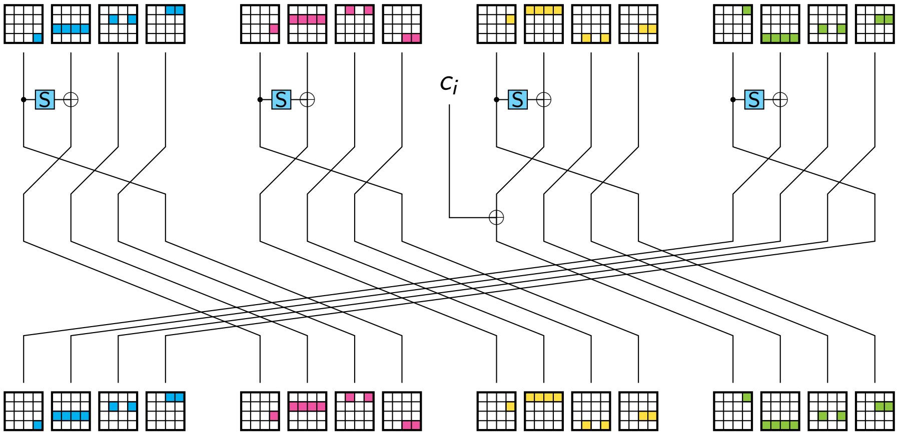
Attack		Enc	Verif	Time	Ref
Existential Forgery	Known Plaintext	$2^{110.4}$	2^{102}	$2^{110.4}$	[Wu+, AC'13]
Existential Forgery	Known Plaintext	2^{103}	2^{103}	2^{104}	[KR, SAC'14]
Existential Forgery	Known Plaintext	1	2^{120}	2^{120}	[KR, SAC'14]
State Recovery, Almost Univ. Forgery	Known Plaintext	1	2^{121}	2^{121}	[KR, SAC'14]
State Recovery, Almost Univ. Forgery	Chosen Plaintext	$2^{57.3}$	0	$2^{104.4}$	New

Comparison of attacks against ALE.

Table of contents

Table of contents

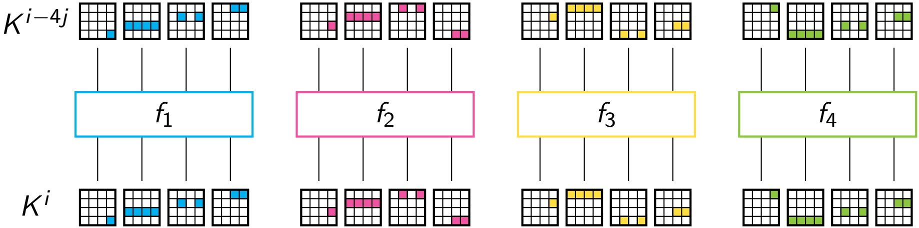
Property on the AES Key Schedule



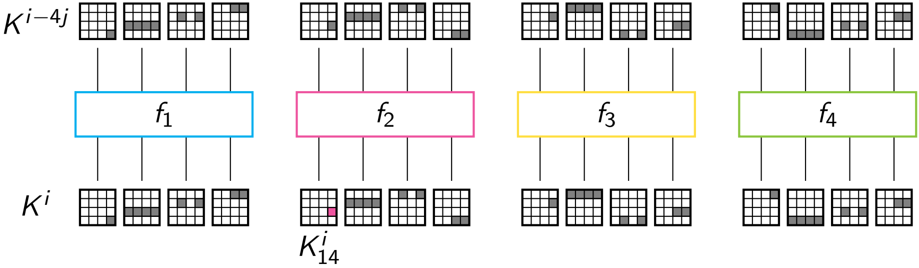
One round of the AES key schedule with graphic representations of bytes positions (alternative representation).

Only the XOR of the colored bytes is required for each state.

Property on the AES Key Schedule

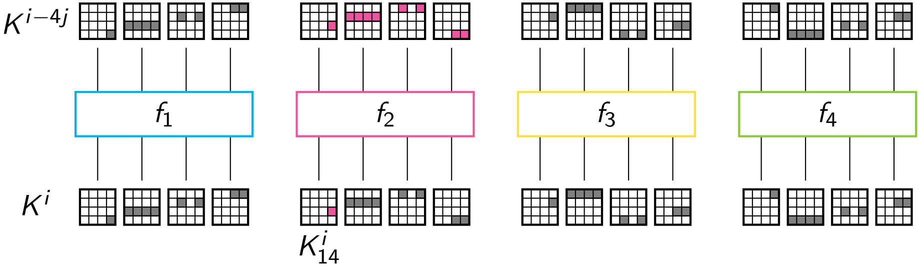


Property on the AES Key Schedule



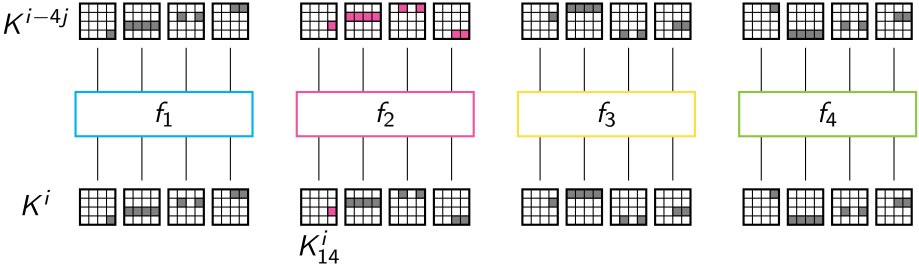
How to compute K^i_{14}?

Property on the AES Key Schedule



How to compute K^i_{14}?

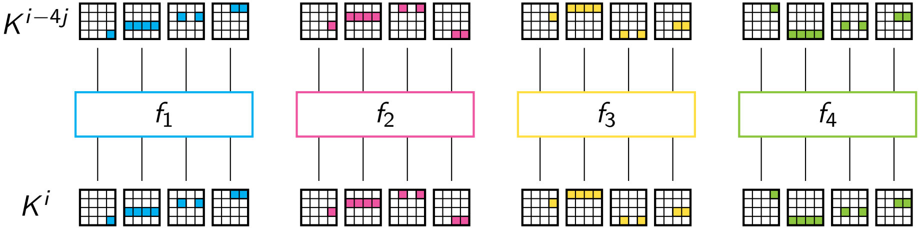
Property on the AES Key Schedule



How to compute K^i_{14}?

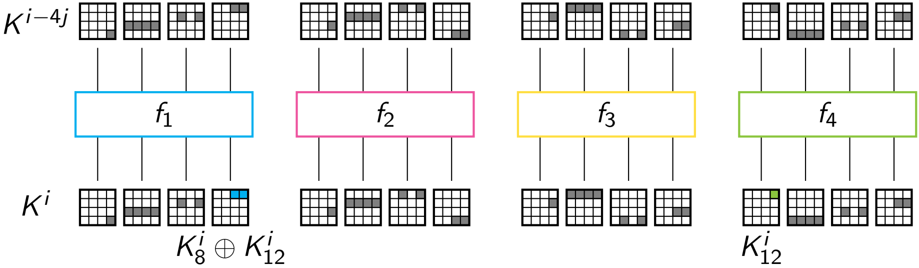
→ **A byte in the last column depends on only 32 bits of information.**

Property on the AES Key Schedule



$\rightarrow$ A byte in the last column depends on only 32 bits of information.

Property on the AES Key Schedule

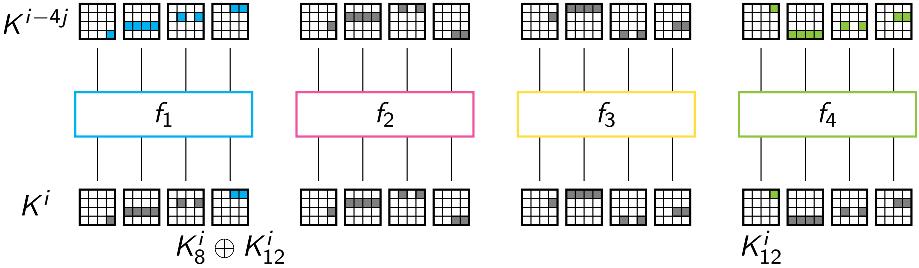


How to compute K_8^i?

$$K_8^i = (K_8^i \oplus K_{12}^i) \oplus K_{12}^i$$

$\rightarrow$ A byte in the last column depends on only 32 bits of information.

Property on the AES Key Schedule

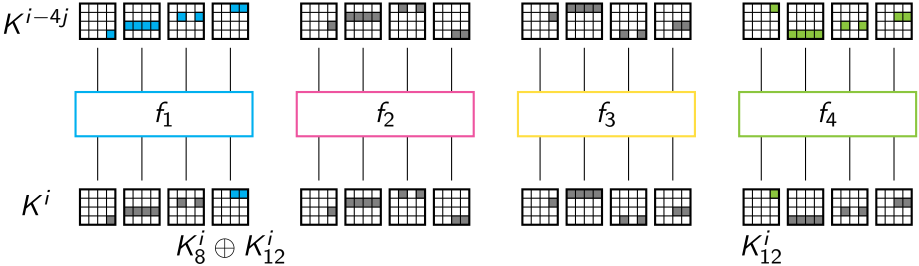


How to compute K_8^i?

$$K_8^i = (K_8^i \oplus K_{12}^i) \oplus K_{12}^i$$

$\rightarrow$ A byte in the last column depends on only 32 bits of information.

Property on the AES Key Schedule



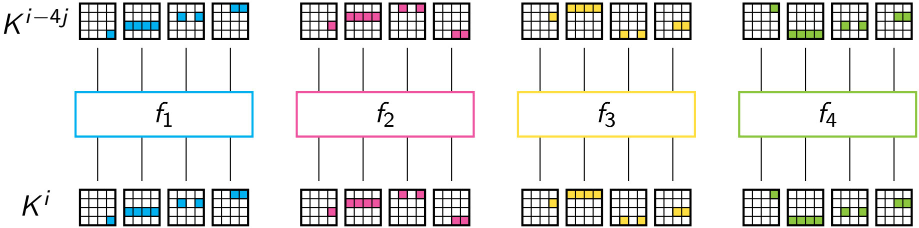
How to compute K_8^i?

$$K_8^i = (K_8^i \oplus K_{12}^i) \oplus K_{12}^i$$

→ A byte in the last column depends on only 32 bits of information.

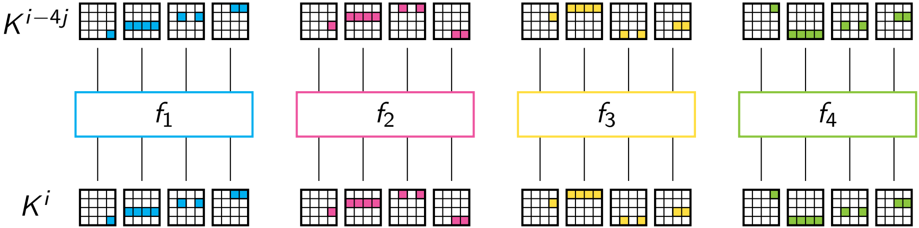
→ **A byte in the 3rd column depends on only 64 bits of information.**

Property on the AES Key Schedule



→ A byte in the last column depends on only 32 bits of information.
→ A byte in the 3rd column depends on only 64 bits of information.
→ **A byte in the 2nd column depends on only 64 bits of information.**

Property on the AES Key Schedule



$\rightarrow$ A byte in the last column depends on only 32 bits of information.
$\rightarrow$ A byte in the 3rd column depends on only 64 bits of information.
$\rightarrow$ A byte in the 2nd column depends on only 64 bits of information.
$\rightarrow$ **A byte in the first column depends on 128 bits of information.**

Property on the AES Key Schedule

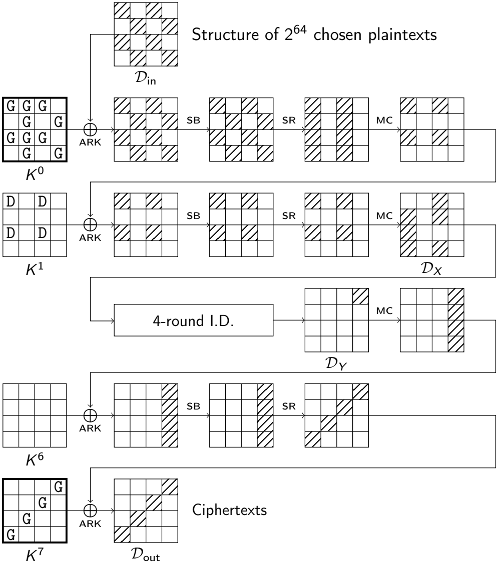
Using our **new representation** of the key schedule, we demonstrate that:

- $\rightarrow$ A byte in the **last** column depends on only **32 bits** of information
- $\rightarrow$ A byte in the **3rd** column depends on only **64 bits** of information
- $\rightarrow$ A byte in the **2nd** column depends on only **64 bits** of information
- $\rightarrow$ A byte in the **first** column depends on **128 bits** of information

Even after a large number of rounds, the key schedule does not mix all the bytes!

Table of contents

Impossible Differential – AES



7-round impossible differential attack ([MDRM, IC'10]).
Figure adapted from Tikz for Cryptographers [Jean].

The attack is in 2 parts:

(1) find candidates for the key bytes marked G.

(2) find the master keys corresponding to these bytes.

Matching bytes from K^0 and K^7

Given 10 bytes of K^0 and 4 bytes of K^7,
how to find the corresponding master keys?

Matching bytes from K^0 and K^7

Given 10 bytes of K^0 and 4 bytes of K^7,
how to find the corresponding master keys?

Naively:

- Guess 6 bytes of K^0
- Filter using 4 bytes of K^7

Complexity: 2^{48}

Matching bytes from K^0 and K^7

Given 10 bytes of K^0 and 4 bytes of K^7,
how to find the corresponding master keys?

Naively:

- Guess 6 bytes of K^0
- Filter using 4 bytes of K^7

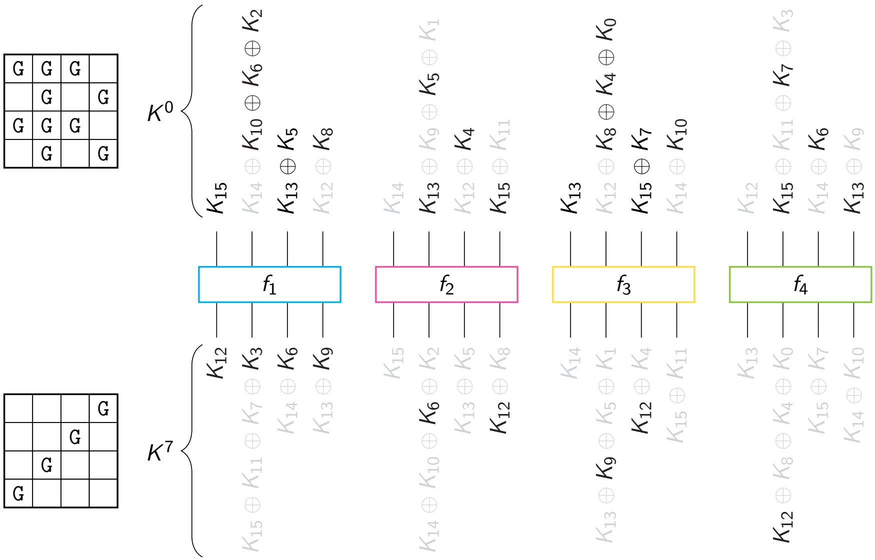
Complexity: 2^{48}

Improvement:

- Guess 2 bytes of K^0
- Filter using 2 bytes of K^7
- Guess 2 bytes of K^0
- Filter using 1 byte of K^7
- Guess 1 byte of K^0
- Deduce 1 byte of K^0 from K^7

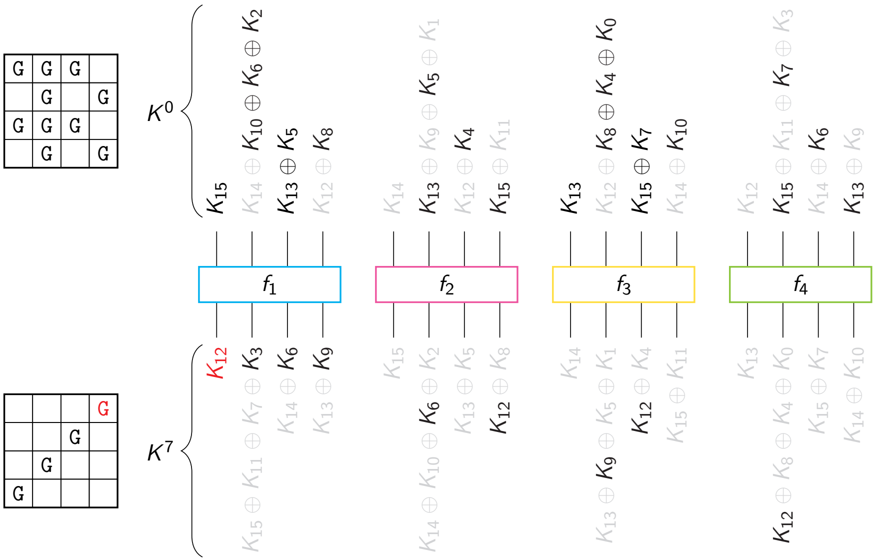
Complexity: 4×2^{16}

Matching bytes from K^0 and K^7



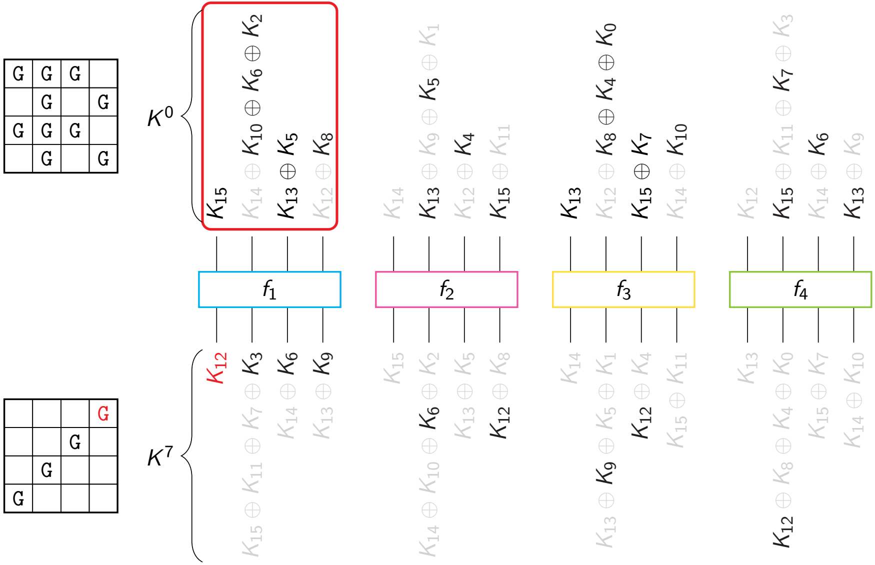
Matching bytes from K^0 and K^7

How to compute K^7_{12} from K^0?



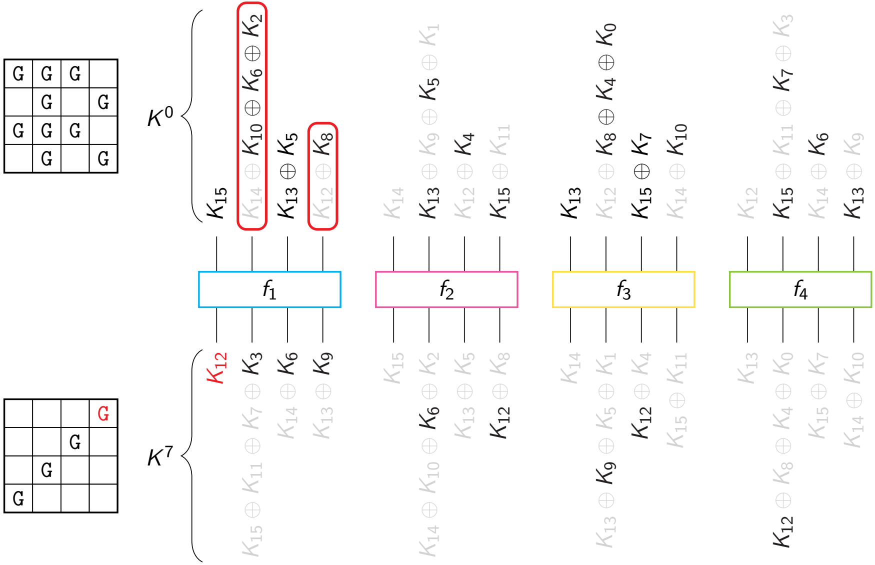
Matching bytes from K^0 and K^7

How to compute K^7_{12} from K^0?



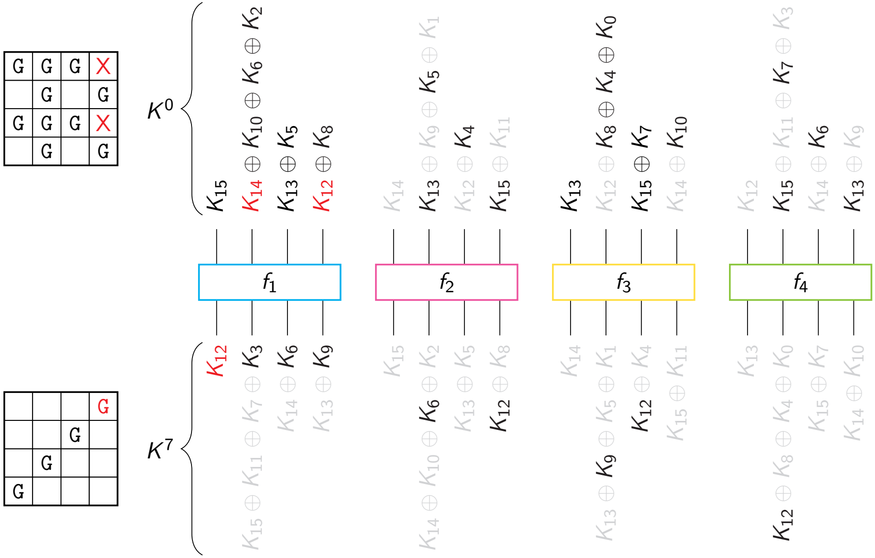
Matching bytes from K^0 and K^7

How to compute K^7_{12} from K^0?

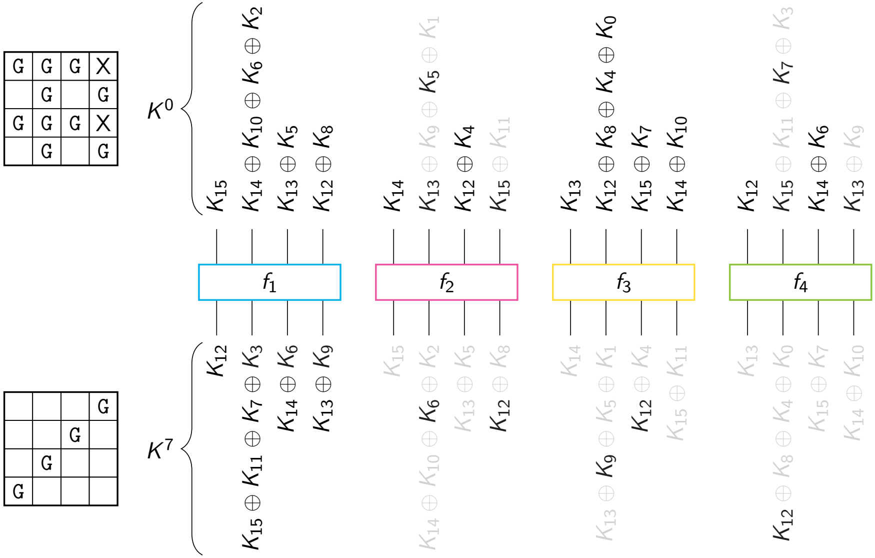


Matching bytes from K^0 and K^7

We can filter using K^7_{12} by guessing only 2 bytes of K^0!

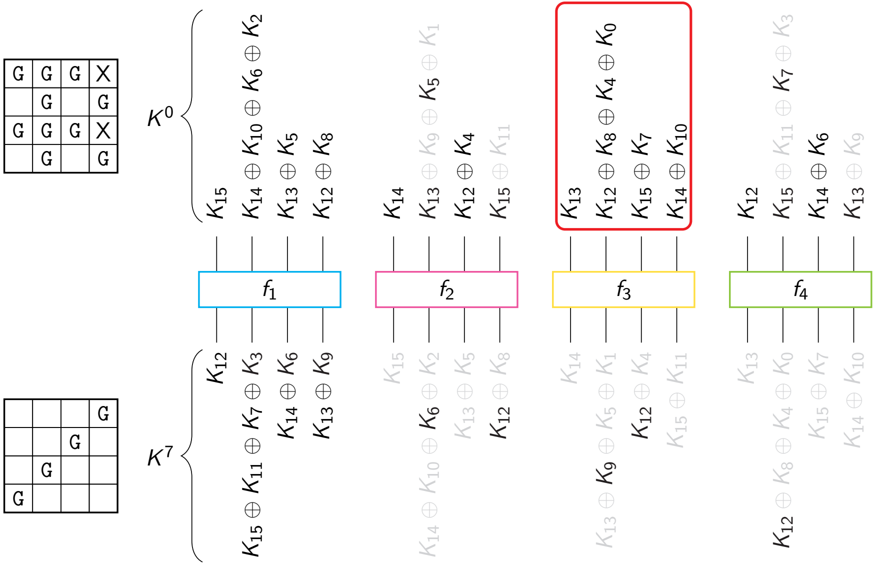


Matching bytes from K^0 and K^7



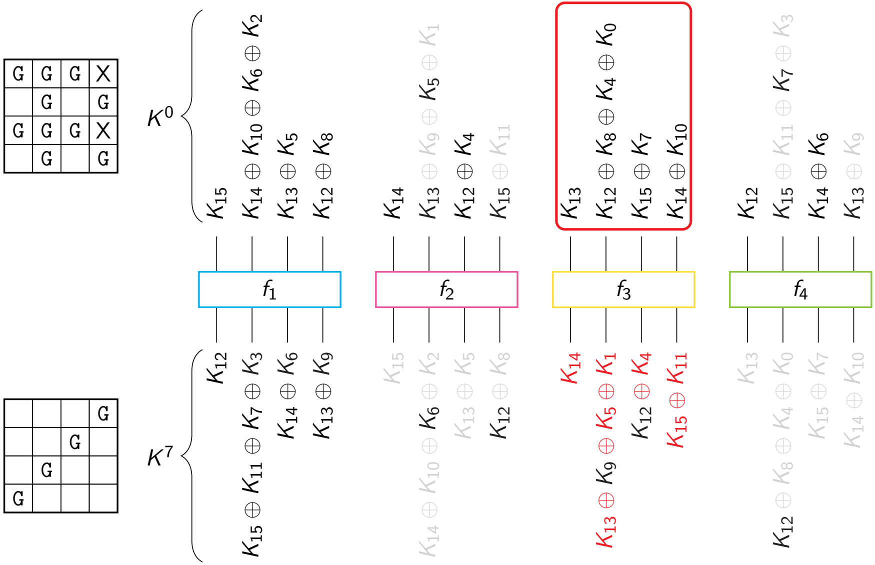
Matching bytes from K^0 and K^7

All the input of f_3 is known, so the output is also known

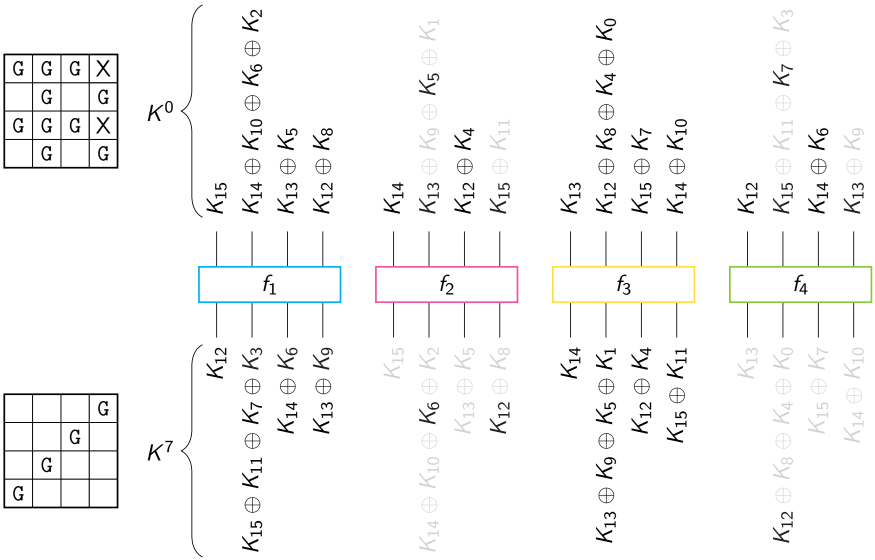


Matching bytes from K^0 and K^7

All the input of f_3 is known, so the output is also known

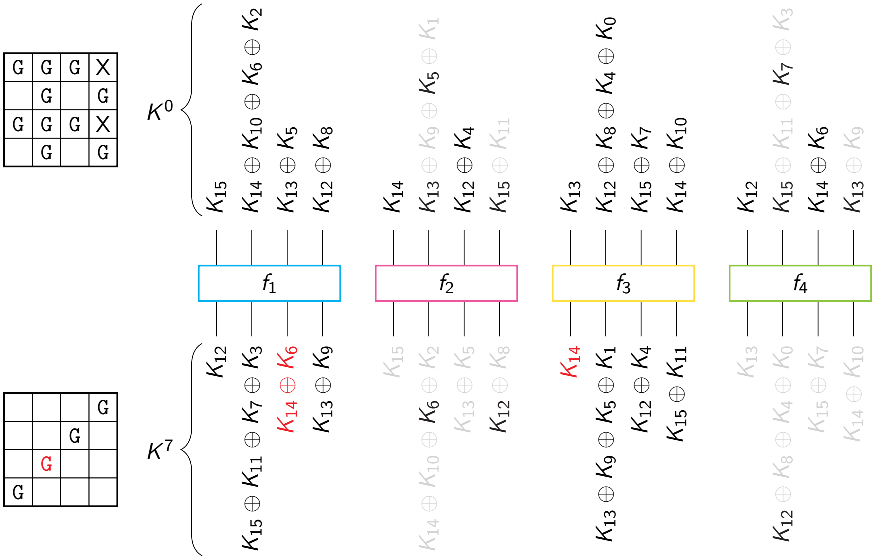


Matching bytes from K^0 and K^7



Matching bytes from K^0 and K^7

We are also able to filter according to $K^7_6 = (K^7_{14} \oplus K^7_6) \oplus K^7_{14}$



Results

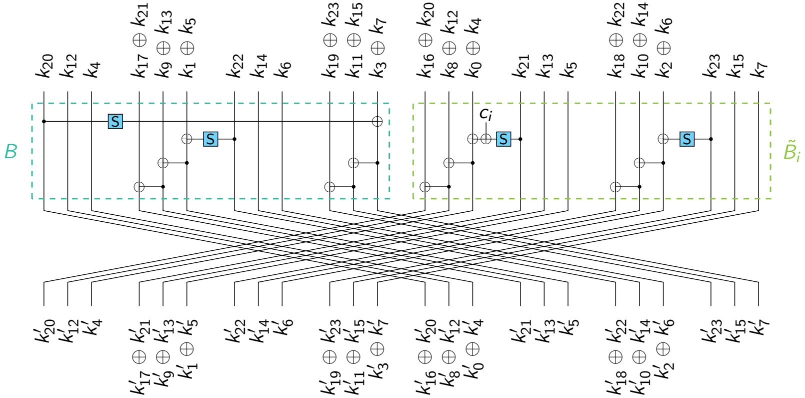
Attack	Data	Time	Mem.	Ref.
Meet-in-the-middle	2^{97}	2^{99}	2^{98}	[Derbez, Fouque, Jean, EC'13]
	2^{105}	2^{105}	2^{90}	[Derbez, Fouque, Jean, EC'13]
	2^{105}	2^{105}	2^{81}	[Bonnetain, Naya-Plasencia, Schrottenloher, ToSC'19]
	2^{113}	2^{113}	2^{74}	[Bonnetain, Naya-Plasencia, Schrottenloher, ToSC'19]
Impossible differential	2^{113}	2^{113}	2^{74}	[Boura, Lallemand, Naya-Plasencia, Suder, JC'18]
	$2^{105.1}$	2^{113}	$2^{74.1}$	[Boura, Lallemand, Naya-Plasencia, Suder, JC'18]
	$2^{106.1}$	$2^{112.1}$	$2^{73.1}$	Variant of [Boura, Lallemand, Naya-Plasencia, Suder, JC'18]
	$2^{104.9}$	$2^{110.9}$	$2^{71.9}$	**New**

Best single-key attacks against 7-round AES-128.

Table of contents

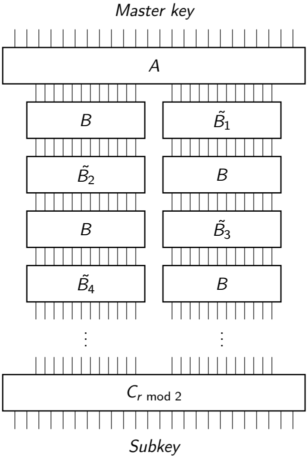
Table of contents

New Representation of the AES-192 Key Schedules



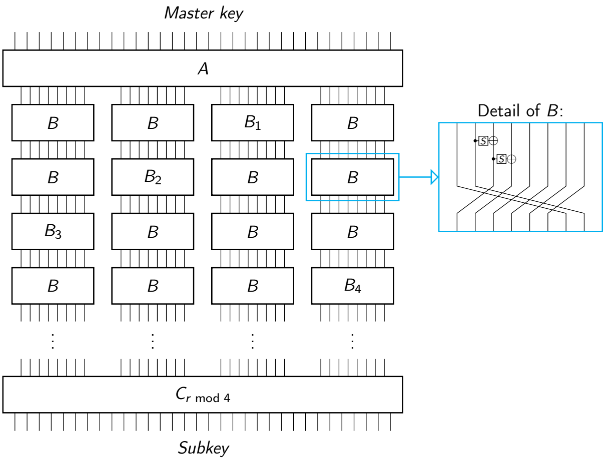
One round of the AES-192 key schedule (alternative representation).

New Representation of the AES-192 Key Schedules



r rounds of the AES-192 key schedule in the new representation.

New Representation of the AES-256 Key Schedules



r rounds of the AES-256 key schedule in the new representation. B_i is similar to B but the round constant c_i is XORed to the output of the first S-box.

Other Results

Attack	Cipher	Rounds	Data	Time	Reference
Square	AES-192	8/12	$2^{128} - 2^{119}$	2^{188}	[FKL+, FSE'00]
			$2^{128} - 2^{119}$	$2^{187.3}$	Variant of [FKL+, FSE'00]
			$2^{128} - 2^{119}$	$2^{185.7}$	Variant of [DKS, AC'10]
			$2^{128} - 2^{119}$	$2^{185.1}$	New
Related-Key Impossible Differential	AES-192	8/12	$2^{64.5}$	2^{177}	[ZWZ+, SAC'06]
			$2^{63.5}$	2^{175}	New
Impossible Differential	Rijndael-256/256	9/14	$2^{229.3}$	2^{194}	[WGR+, ICISC'12]
			$2^{228.1}$	$2^{192.9}$	Variant of [WGR+, ICISC'12]
			$2^{227.6}$	$2^{192.5}$	New
Impossible Differential	Rijndael-256/256	10/14	$2^{244.2}$	$2^{253.9}$	[WGR+, ICISC'12]
			$2^{243.9}$	$2^{253.6}$	Variant of [WGR+, ICISC'12]
			2^{242}	$2^{251.7}$	New

Square Attack

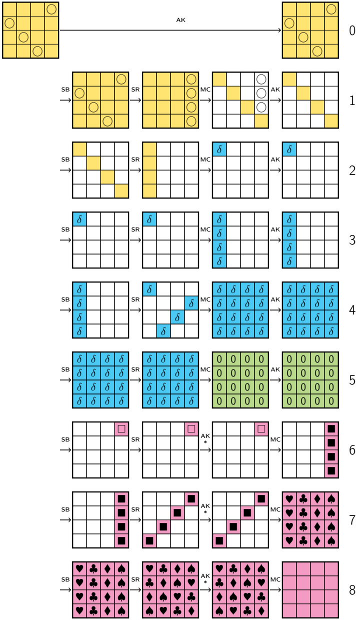
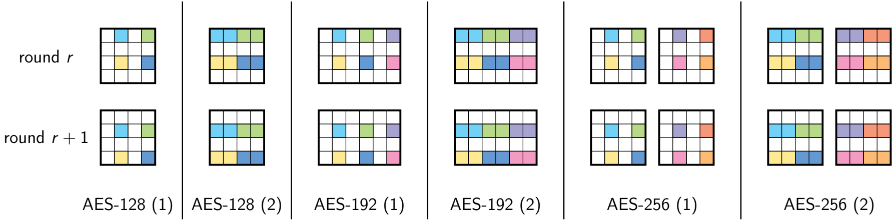


Table of contents

Properties on the AES Key Schedule



Representation of the position of the bytes of the proposition.

In cases (2), only the XOR of the two bytes of the same color must be known.

Table of contents

Conclusion

→ **Alternatives representations** of AES key schedules:

- 128 bits: 4 chunks of 4 bytes
- 192 bits: 2 chunks of 12 bytes
- 256 bits: 4 chunks of 8 bytes

Conclusion

→ **Alternatives representations** of AES key schedules:

- 128 bits: 4 chunks of 4 bytes
- 192 bits: 2 chunks of 12 bytes
- 256 bits: 4 chunks of 8 bytes

→ **Attacks on mixFeed and ALE**: they exploit the presence of short length cycles when iterating an odd number of rounds of key schedule.

Conclusion

→ **Alternatives representations** of AES key schedules:

- 128 bits: 4 chunks of 4 bytes
- 192 bits: 2 chunks of 12 bytes
- 256 bits: 4 chunks of 8 bytes

→ **Attacks on mixFeed and ALE**: they exploit the presence of short length cycles when iterating an odd number of rounds of key schedule.

→ **Improvement of Impossible Differential** and **Square** attacks against the **AES** by **combining efficiently** information from subkeys.

Conclusion

→ **Alternatives representations** of AES key schedules:

- 128 bits: 4 chunks of 4 bytes
- 192 bits: 2 chunks of 12 bytes
- 256 bits: 4 chunks of 8 bytes

→ **Attacks on mixFeed and ALE**: they exploit the presence of short length cycles when iterating an odd number of rounds of key schedule.

→ **Improvement of Impossible Differential** and **Square** attacks against the **AES** by **combining efficiently** information from subkeys.

→ It confirms that the key schedule should not be considered as a random permutation.

Conclusion

→ **Alternatives representations** of AES key schedules:
- 128 bits: 4 chunks of 4 bytes
- 192 bits: 2 chunks of 12 bytes
- 256 bits: 4 chunks of 8 bytes

→ **Attacks on mixFeed and ALE**: they exploit the presence of short length cycles when iterating an odd number of rounds of key schedule.

→ **Improvement of Impossible Differential** and **Square** attacks against the **AES** by **combining efficiently** information from subkeys.

→ It confirms that the key schedule should not be considered as a random permutation.

For more details:

`https://eprint.iacr.org/2020/1253`