A Method for Security Estimation of the SPN-Based Block Cipher Against Related-Key Attacks

Vera Shilina

Samara University

Contents

Introduction

To prove the security of an encryption algorithm against related-key attacks it is needed to find the best differential characteristic. The best characteristic has as few active bytes as possible. So, to find the best differential characteristic the amount of active bytes, which will be used during its construction, should be counted. An active byte is a non-zero byte difference that passes through the substitution table.

Objective: To develop a method for security estimation of the SPN-based block cipher against related-key attacks, focusing on vulnerabilities identified in the key expansion scheme. The method is based on the algorithm for counting active bytes.

A prospective SPN-based block cipher

A prospective SPN-based block cipher

This cipher is based on AES. The main differences compared to AES are the follows: pre- and post-whitening use modulo addition 2^{64}, expanded size of MDS matrix to 8×8, application of several S-boxes optimized with respect to differential, linear and algebraic cryptanalysis, and considerably redesigned key expansion routine.

Basic transformations

In the presented algorithm four basic transformations are used:

- key addition;
- bytes substitution;
- shift rows;
- mix columns.

These transformations are the basis of entire high-level structure.

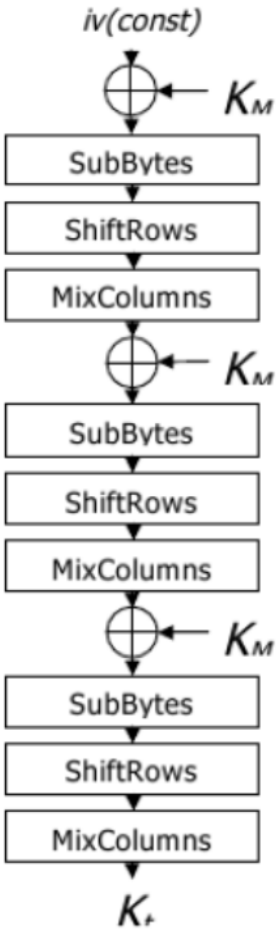
Key expansion scheme

The key expansion scheme contains the following two steps:

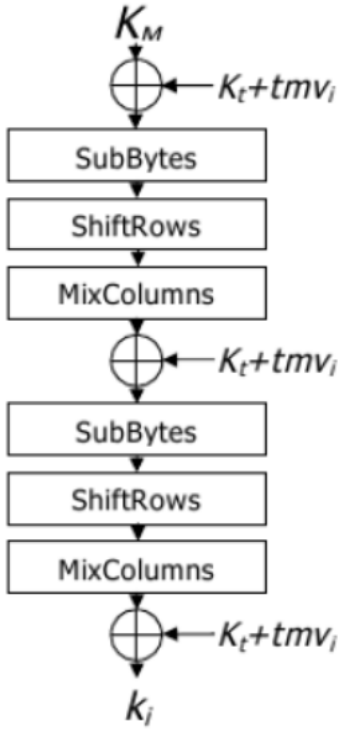
Computing of an intermediate value K_t based on a master key K_M and constants.

Computing of round keys (K_1, K_2, ..., K_m) based on a master key K_M, an intermediate value K_t and constants.

Key expansion scheme

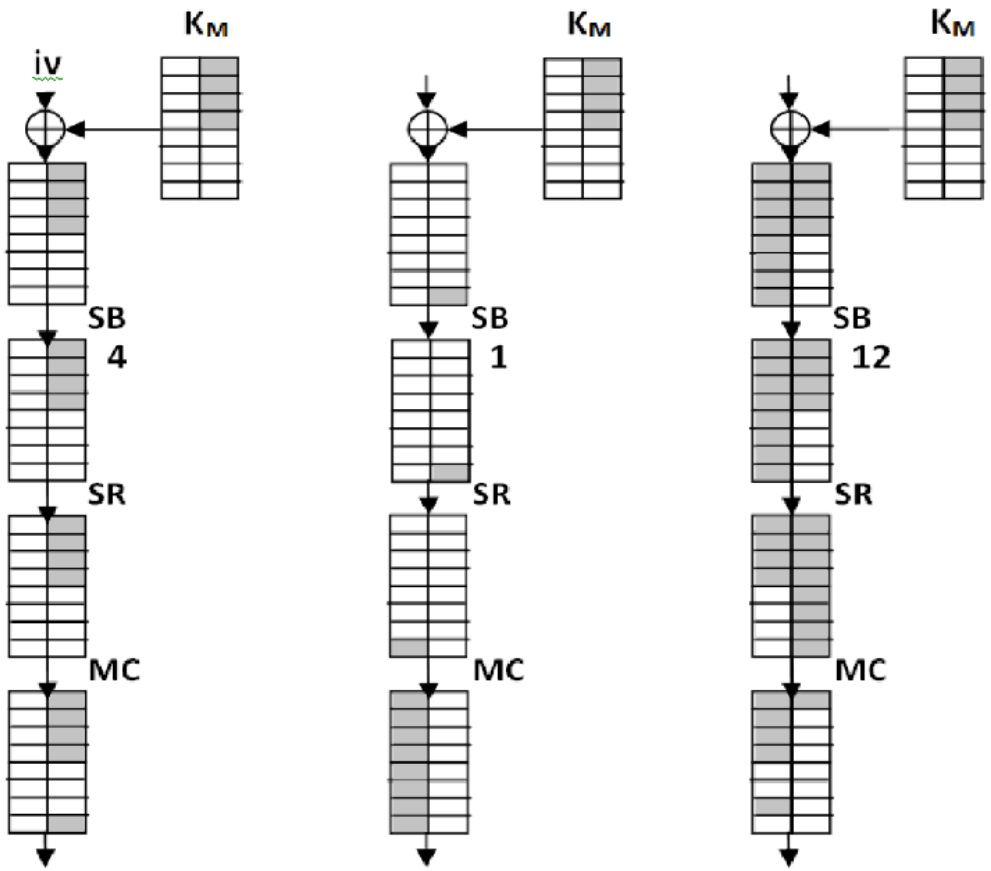


Computing of K_t



The computation of round keys

The algorithm for counting active bytes

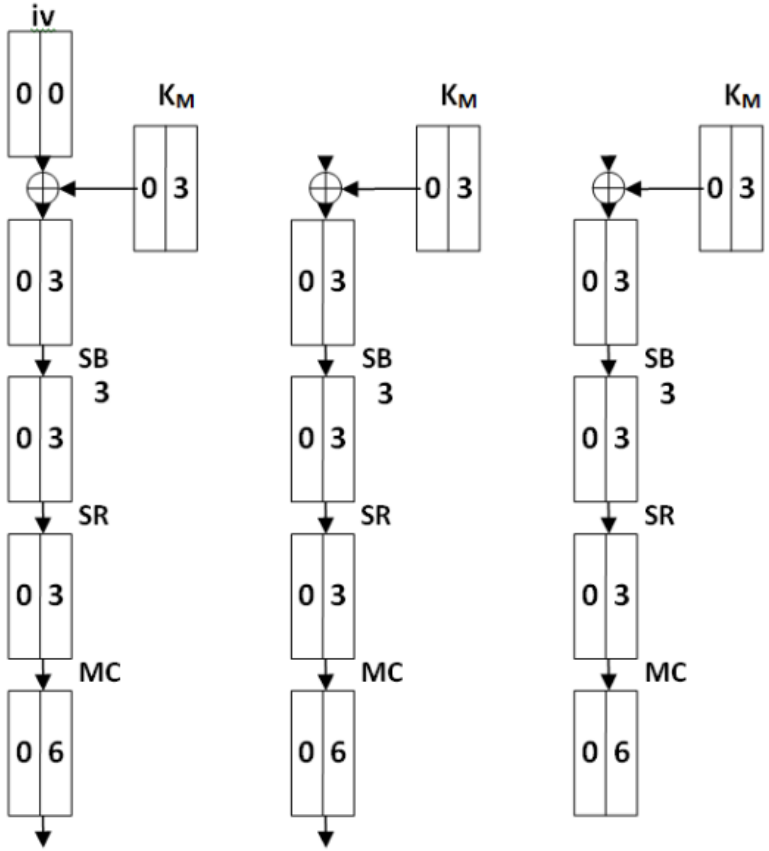


A differential trail for K_t computation

In the proposed method the entire column is under control instead of separate bytes.
Symbols:
iv – the difference of initial vectors (always equal to zero);
K_M – master key of encryption (which is needed to be expanded);
SB – sub bytes (bytes substitution using substitution tables);
SR – shift rows;
MC – mix columns.

The algorithm for counting active bytes

The non-zero numbers (i.e., active bytes) are recalculated after each transformation.



An example of the active bytes computation

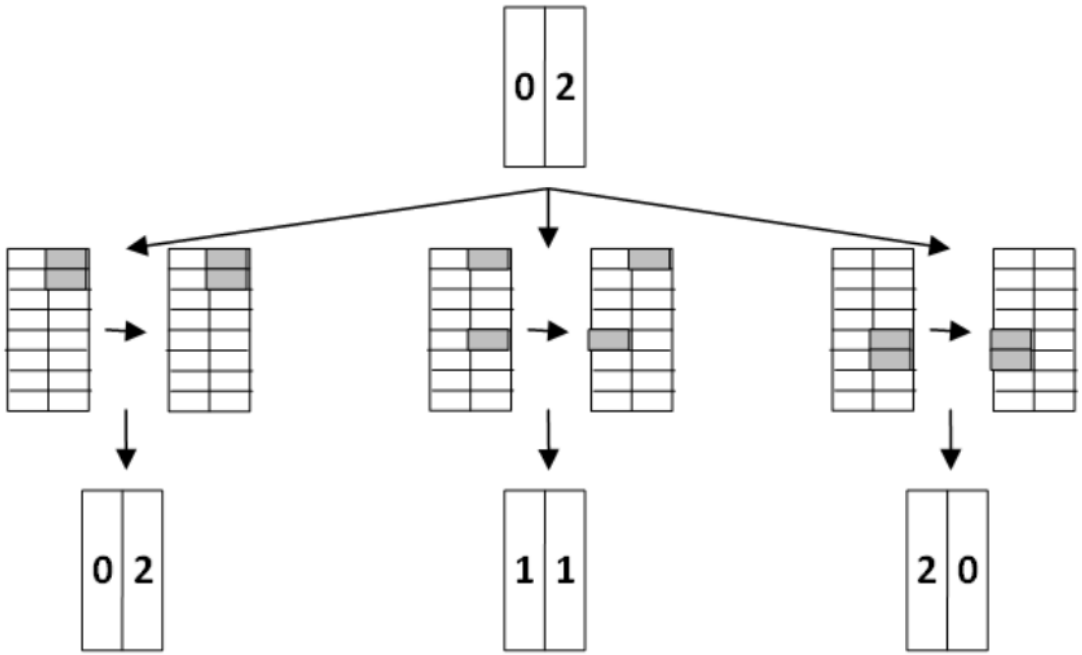
Key addition, Byte substitution

The key addition operation is performed as follows: a value of a state column is subtracted from a value of the corresponding column of a key state. Then an absolute value of the result is taken.

The byte substitution transformation does not change the amount of non-zero bytes. The value is always constant before and after the transformation.

Shift rows

The differential trail can be branched. It takes a lot of computational resources, because in each round new branches appear and the amount of these independent branches is growing exponentially.



The calculation of active bytes after shift rows for the proposed algorithm

Shift rows

The total amount of branches after the shift rows transformation will not exceed the product of possible shifts of the left column and the right column.

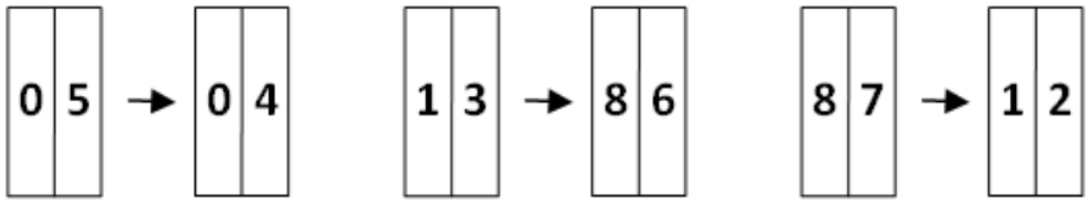
Amount of non-zero bytes in a column	Amount of branches
0	1
1	2
2	3
3	4
4	5
5	4
6	3
7	2
8	1

The amount of branches depends on the amount of non-zero bytes in a column

Mix columns

Mixing in columns is performed as the product of column and a fixed matrix. Unlike the previous one this transformation does not create new branches. The main property of the mix columns transformation is the sum of non-zero bytes on the input and the output cannot be less than 9:

$$N_{in} + N_{out} \geq 9.$$



The calculation of active bytes after mix columns

The description of results

The minimal secure threshold for estimated cipher is 26 active bytes. This value is obtained from the next equation:

$$(2^{-5})^x < 2^{-128},$$

where 2^{-128} is the probability to break the cipher with the brute force attack, 2^{-5} is the maximum probability that an input difference maps to the output difference. Therefore, for 26 active bytes the entire complexity to break the cipher is 2^{-130}, which is more than the complexity of the brute force attack.

The description of results

The main property of the searching algorithm is that the exact trail cannot be found, but one can prove that the encryption algorithm is resistant against related-key attacks. In particular, if the number of active bytes is greater than or equal to the threshold then it is impossible to find a differential trail that can be used in an differential attack.

Conclusions

Thus, the proposed method gives an analytic proof of the security of block ciphers regarding related-key attacks. It was shown that the 128-bit version of the cipher does not have a differential characteristic that can lead to the key recovery attack with complexity lower than the complexity of the brute force attack.
This method can be extended to different variants of block size and key lengths of the proposed cipher as well as to other block ciphers with the similar structure.