Security Analysis

In this section, we provide an in-depth analysis of the security of the SKINNY family of block ciphers. These models are based on related-key models.

Integral attack:-
In this attack, we prepare a set of plaintext, so that particular cells can contain all the value in the set,and other cells are fixed to a constant ,after several round of encryption, we see the changes of this encryption.For this we consider four properties All,Balanced,constant,unknown. Definition of these for all following.
All :- same number appear in the all cell.
Balance :- The sum of all values in the multiset is 0.
constant :- The cell value is fixed through the multiset.
unknown. :- No particular property exists

.....image1.....

Now we will find the maximum number of rounds, so that we get any non-trivial properties.For this we do or follow an Experiment.Initially we set only one active cell to the state. And encrypt until we all cells become Unknown and in the process, we use different values of constant cells and tweakey.

As a result, we found that an active cell in any of the third row will yield two cells satisfying the property after seven rounds.

property is extended to higher order by changing active cells in the backward direction.
Ex:- property can be extended by 4 round in backwards by activating 12 cells and in the end we get 10 round integral distinguisher can be constructed
.....image 2.....

We take about algebraic degree of the 4-bit sbox and 8 bit sbox, Then in 4 bit sbox algebraic degree is 3 while 8 bit sbox is 6.Thus the integral property of Skinny 128 can be longer than Skinny.Now we see how these three properties help us to recover 4 rounds.After the 10-round integral distinguisher we go 4 rounds in forward.So that we will attack on backward and reach 10-round .
process(Follow figure):-
1)First we prepares 2^12c plaintext for integral distinguisher.After that we compute inverse MixColumns for each ciphertext.then we change 4-cell values for proceed backward computation.Now we have 8 active cell.Now our remaining text size is 2^8c.

2)Actually we are going backward, so we know all the ciphertext, in 13 rounds we again invers SubCells and MixColumns.we can see in the figure we again change 4 cells to our properties. In this step guess data and compute, before this we have 2^8c data. For this we perform 2^8c . 2^4c = 2^12c.Now our remaining text size is 2^5c.

3) Given 2^5c data,we again compute inverse MixColumns in round-12 for each ciphertext.then we change 2-cell values for proceed backward computation. For this we need 2^6c guesses. which requires 2^11c computation.

4) Given 2^2c data,we again compute inverse MixColumns in round-11 for each ciphertext.then we change 1-cell values to proceed backward computation.

5)Computed results are tested if the Balanced (B) property is satisfied. The guessed 10-cell key candidates are reduced by a factor of 2^−3c
.
So memory, data, computation required in this attack are following
memory 2^12c , data 2^12c,computation 2^12c)

where c is the size of the cell.

----------image 3 start

Impossible Differential Attacks:-

In this attack, attackers find two internal state differences, where both states never propagate to each other.
like if we have two states \del and \del', the \del is never propagated to \del' other.
After that the attacker finds many plain text and ciphertext and tweakey values, those are leading to (\del , \del'). If any tweakey value is wrong, then we will reduce from tweakey space.

Basically in this analysis ,with the help of miss-in-the-middle We find impossible differential characteristics technique , for these we took 16 input truncated differentials and 16 output truncated differentials with single active cells propagated with encrypt and decrypt function. and Until no cell can be active or inactive with probability one, then we pick up the pair contradicting each other in the middle.

And in the end we get the longest impossible differential characteristics to reach 11 rounds with 16 such characteristics in total.
(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, ∆, 0, 0, 0) 12R -> cut (0, 0, 0, 0, 0, 0, 0, 0, ∆0
, 0, 0, 0, 0, 0, 0, 0).
And we can also add several round before and after the 11 round impossible differential characteristics, and number of round depend on key size, if block size and key size are same then after add two round before and three round after, we get plaintext differences
s (0, 0, 0, ∗, ∗, ∗, ∗, 0, 0, ∗, 0, ∗, 0, 0, ∗, 0) and the ciphertext difference becomes and the ciphertext difference becomes (∗, ∗, ∗, ∗, ∗, ∗, ∗, 0, 0, 0, ∗, ∗, ∗, ∗, ∗, 0) where * is non-zero different.

----------figure 3 ----------

In this Cipher AddroundTweakey, shiftrow and Mixcolumn are effect on each other between different states.
And the number of tweakey cells involved is 3 in the first tree round while 5 in the last tree round. So 8 cells in total.

Meet-In-The-Middle Attacks :-
This attack has been applied to block ciphers. Basically it works on SPN structure. we only see some definition or process.Not a proof.
According to this Number of attacked rounds can be calculated by considering the maximum length of three features.

a)Partial-Matching :- If Number of rounds reaches full diffusion rounds in both directions(backward and forward). In SKINNY full diffusion is achieved after 6 rounds forward and backward.
then Partial-Matching on work at most 10 ((6-1)+(6-1)) rounds.

b)Initial structure :- This structure can also be bounded by a smaller number of full diffusion rounds in both directions(backward and forward).
and it works up to 7 (6+2-1) rounds for SKINNY.

c)Splice-and-cut :- It is also the same as Initial structure, and it may extend the Number of rounds up to the same number of full diffusion rounds minus one (means 6-1=5). And it the end, we get a total 10+7+5=22 round from Meet-In-The-Middle Attacks.

So we can say 32+ rounds of SKINNY can provide a valuable security margin.