Related-Key Impossible-Differential Attack on Reduced-Round SKINNY

Ralph Ankele[1], Subhadeep Banik[2], Avik Chakraborti[3], Eik List[4], Florian Mendel[5], Siang Meng Sim[2], Gaoli Wang[6]

[1]Royal Holloway, University of London, UK [2]Nanyang Technological University, Singapore
[3]Indian Statistical Institute, India [4]Bauhaus-Universitaet Weimar, Germany [5]Graz University of Technology, Austria [6]East China Normal University, China

January 20, 2017

Early Symmetric Crypto 2017, Canach, Luxembourg

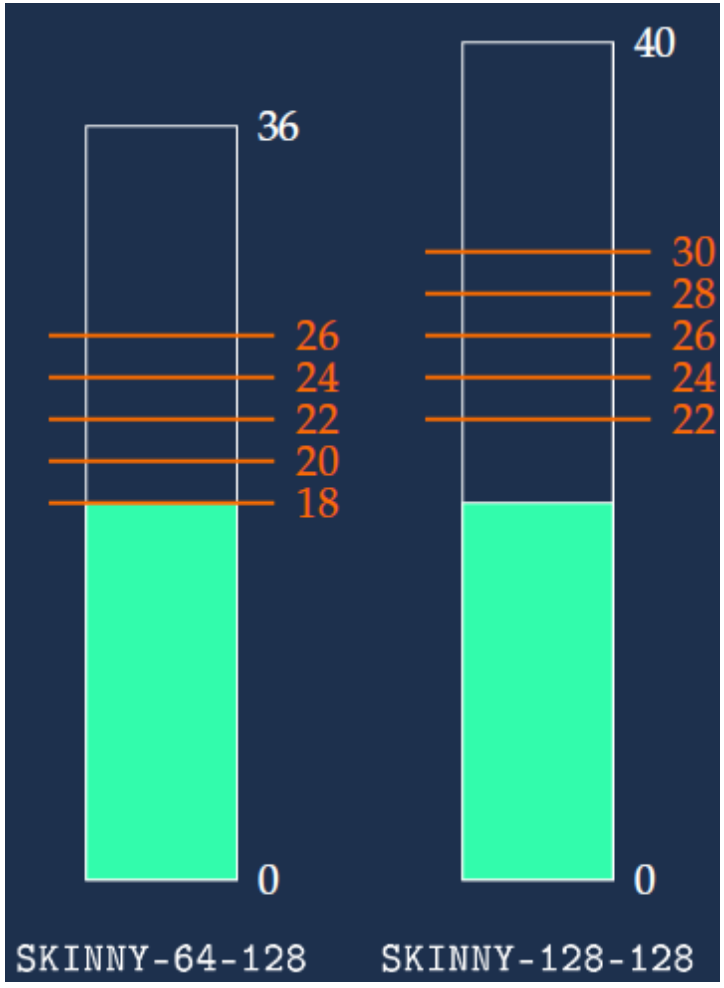
Ralph Ankele has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 643161

Motivation

- SIMON [BSS+13] is considered for standardization for ISO 29192-2
  - × Design by NSA
  - × No design rational (in contrast to common behaviour)
  - × No security analysis by the designers
  - × Based on not well understood AND-RX structure
  - ✓ ... but, good software performance
  - ✓ and lots of cryptanalytic results
- SKINNY [BJK+16b]
  - ✓ Design by academic team
  - ✓ Detailed design rational
  - ✓ Detailed security analysis by designers
  - ✓ Based on well understood components
  - ✓ Good performance in software/hardware

Motivation

SKINNY competition [BJK+16a]



Our Contributions

Cipher	Rounds	Time Complexity	Attack
SKINNY-64-128	21	2^{86}	Impossible Differential
SKINNY-64-128	21	$2^{71.4}$	Impossible Differential
SKINNY-64-128	22	$2^{71.6}$	Impossible Differential
SKINNY-64-128	23	2^{79}	Impossible Differential

Related Work

[LGL16] Security Analysis of SKINNY under Related-Tweakey Settings

http://eprint.iacr.org/2016/1108

Guozhen Liu and Mohona Ghosh and Ling Song

[TAY16] Impossible Differential Cryptanalysis of Reduced-Round SKINNY

http://eprint.iacr.org/2016/1115

Mohamed Tolba and Ahmed Abdelkhalek and Amr M. Youssef

[SMB16] Cryptanalysis of Reduced round SKINNY Block Cipher

http://eprint.iacr.org/2016/1120

Sadegh Sadeghi and Tahere Mohammadi and Nasour Bagheri

SKINNY

- SKINNY is a family of lightweight tweakable block ciphers
- Based on the STK construction from TWEAKEY framework
- Efficient software/hardware implementations in many scenarios

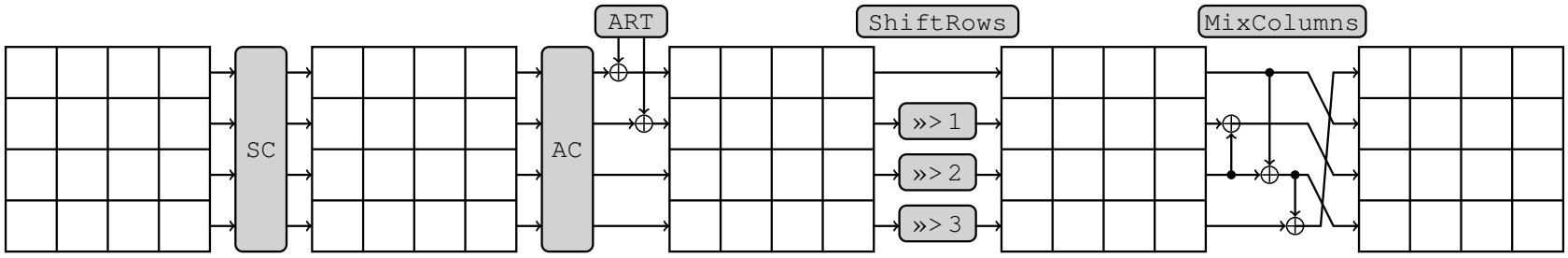
	block size	tweakey size	nr. of rounds
SKINNY-64-64	64	64	32
SKINNY-64-128	64	128	36
SKINNY-64-192	64	192	40
SKINNY-128-128	128	128	40
SKINNY-128-256	128	256	48
SKINNY-128-384	128	384	56

SKINNY

- Skinny has a state of either 64-bit or 128-bit
- Internal State (IS) viewed as a 4 x 4 matrix

$$IS = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & a & b \\ c & d & e & f \end{pmatrix}$$

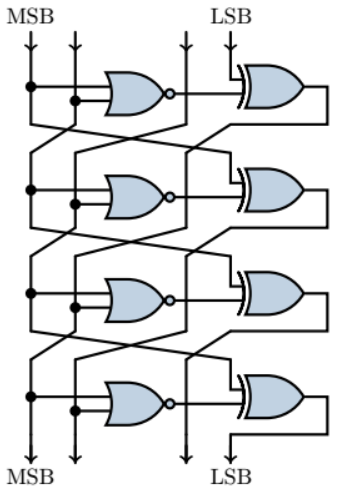
- Round functions:



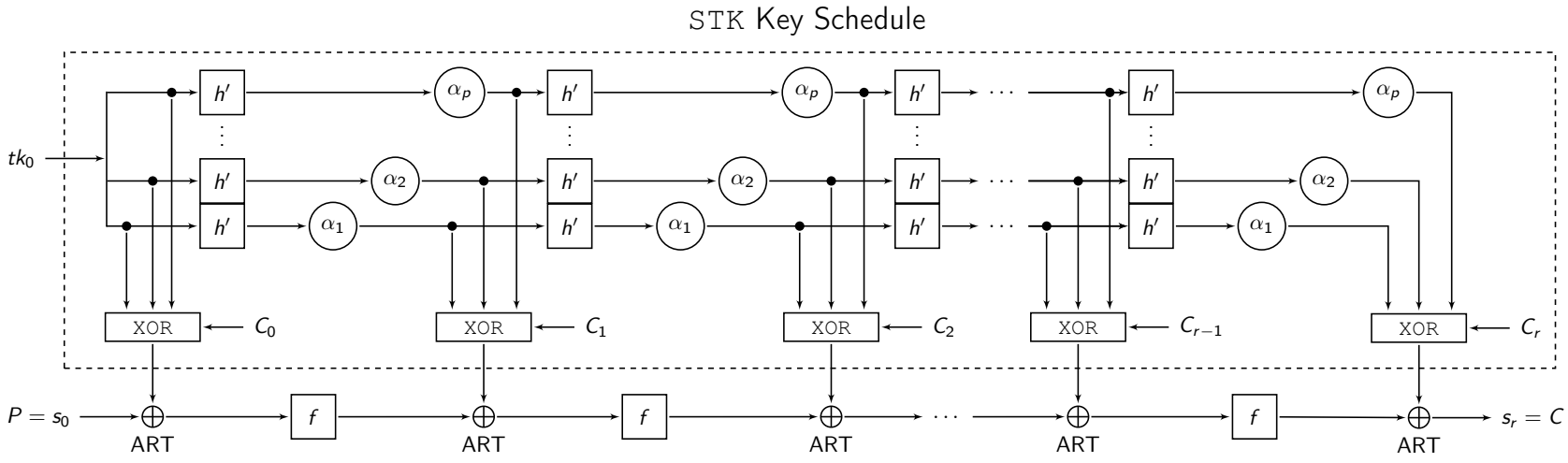
SKINNY

- SubCells (SC): Application of a 4/8-bit SBox to all cells
- AddConstants (AC): Inject round constants into the state
- AddRoundTweakey(ART): Extract and inject the subtweakey into half of the state
- ShiftRows (SR): Right rotate row i by i positions
- MixColumns (MC): Multiply the state with a binary matrix M

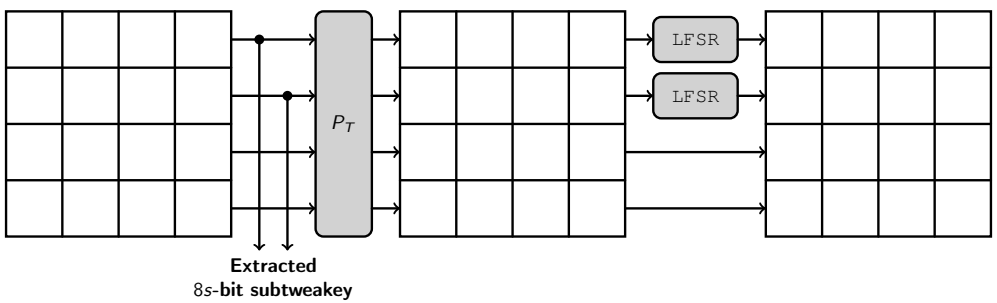
$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$



TWEAKEY schedule in SKINNY

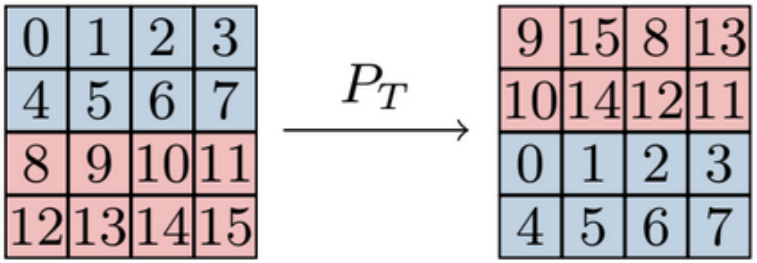


- Based on the STK construction from the TWEAKEY framework [JNP14]
- Only half of the state is XOR'ed to the state
- Tweakey words are updated with permutation P_T and LFSRs



Properties of SKINNY - Tweakey schedule

$$P_T = \begin{pmatrix} 9 & f & 8 & d \\ a & e & c & b \\ 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \end{pmatrix}$$



- Period of $P_T = 16$

TK	LFSR
TK2	$(x_3 \| \| x_2 \| \| x_1 \| \| x_0 \rightarrow x_2 \| \| x_1 \| \| x_0 \| \| x_3 \oplus x_2)$
TK3	$(x_3 \| \| x_2 \| \| x_1 \| \| x_0 \rightarrow x_0 \oplus x_3 \| \| x_3 \| \| x_2 \| \| x_1)$

- Differential cancelation can happen only every 15 rounds for TK2 and two cancelations for TK3

Properties of SKINNY - SBox

Lemma 1

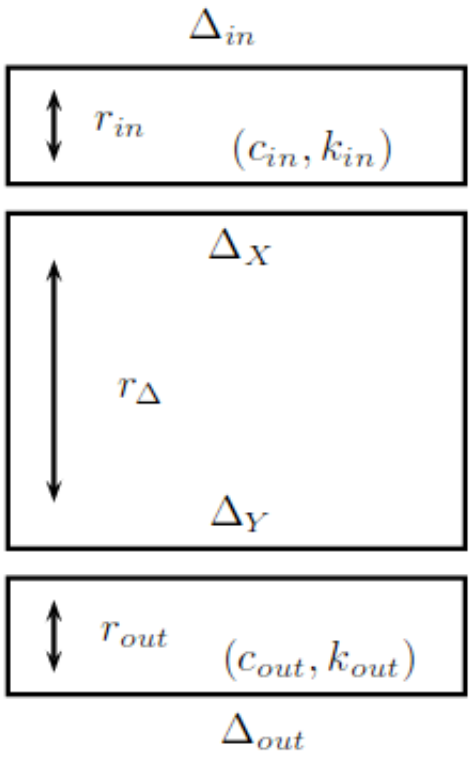
The equation $S(x + \Delta_i) + S(x) = \Delta_o$ has one solution x on average for $\Delta_i, \Delta_o \neq 0$. Similar result hold for the inverse SBox S^{-1}.

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	.	.	.	.	.	.	.	4	4	4	4	.	.	.	.
2	.	4	.	4	.	4	4	.	.	.	.	.	.	.	.	.
3	.	.	.	.	.	.	.	.	2	2	2	2	2	2	2	2
4	.	.	4	.	.	.	2	2	.	.	.	4	2	2	.	.
5	.	.	4	.	.	.	2	2	.	.	4	.	2	2	.	.
6	.	2	.	2	2	.	.	2	2	.	2	.	.	2	2	.
7	.	2	.	2	2	.	.	2	.	2	.	2	2	.	.	2
8	.	.	.	.	4	4	.	.	.	.	.	.	2	2	2	2
9	.	.	.	.	4	4	.	.	.	.	.	.	2	2	2	2
a	.	.	.	.	.	4	4	.	2	2	2	2	.	.	.	.
b	.	4	.	4	.	.	.	.	.	.	.	.	2	2	2	2
c	.	.	4	.	.	.	2	2	4	.	.	.	.	.	2	2
d	.	.	4	.	.	.	2	2	.	4	.	.	.	.	2	2
e	.	2	.	2	2	.	.	2	.	2	.	2	.	2	2	.
f	.	2	.	2	2	.	.	2	2	.	2	.	2	.	.	2

The average can be calculated as:

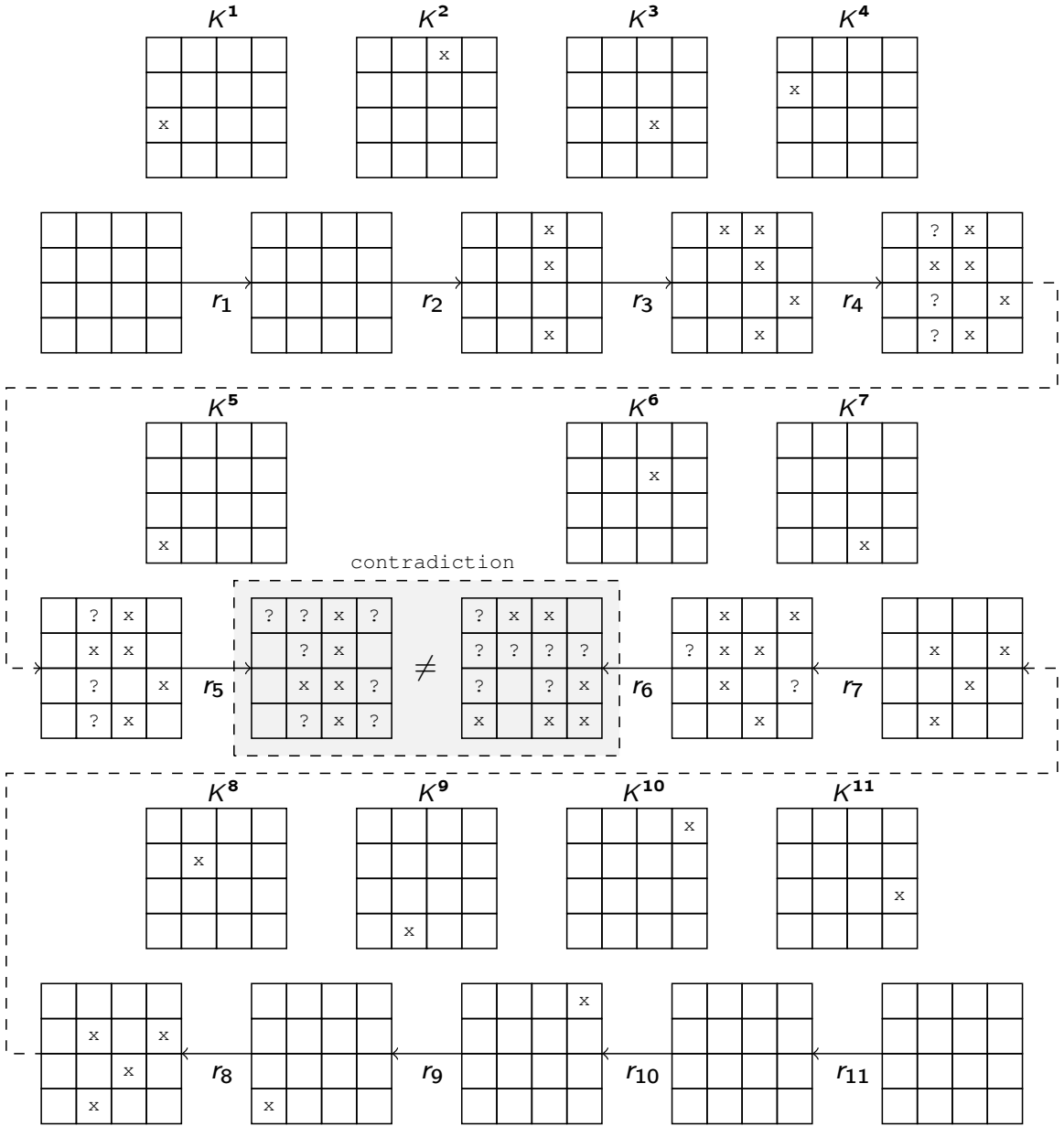
$$\frac{1}{225} \cdot \sum_{\Delta_i, \Delta_o \neq 0} DDT(\Delta_i, \Delta_o) \approx 1$$

Impossible Differential Attack



- Independently introduced by Knudsen [Knu98] and Biham et. al. [BBS99] in 1998
- Find a differential with probability zero
- If a plaintext/ciphertext pair is partially encrypted/decrypted to the impossible differential, the guessed key bits are wrong

Impossible Differential Trail



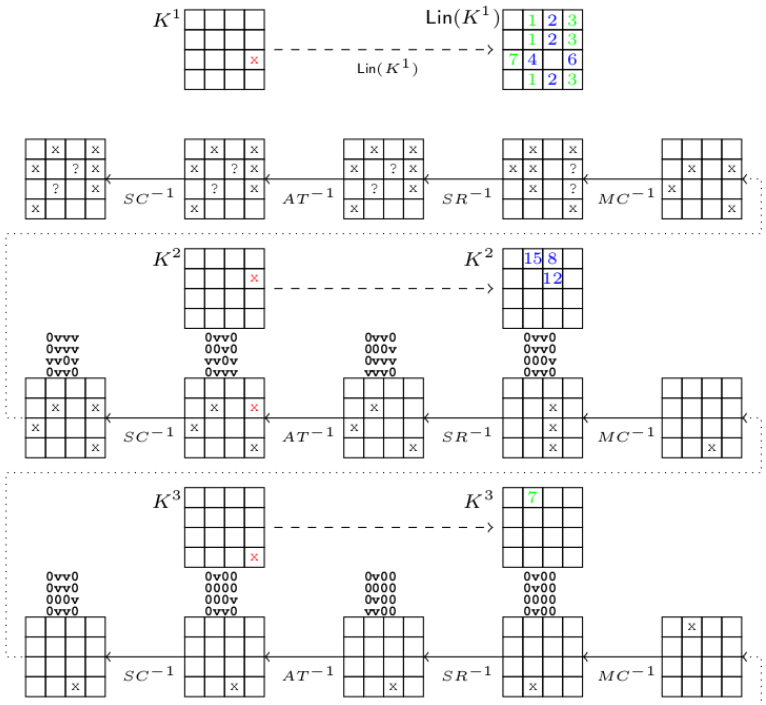
Key Recovery

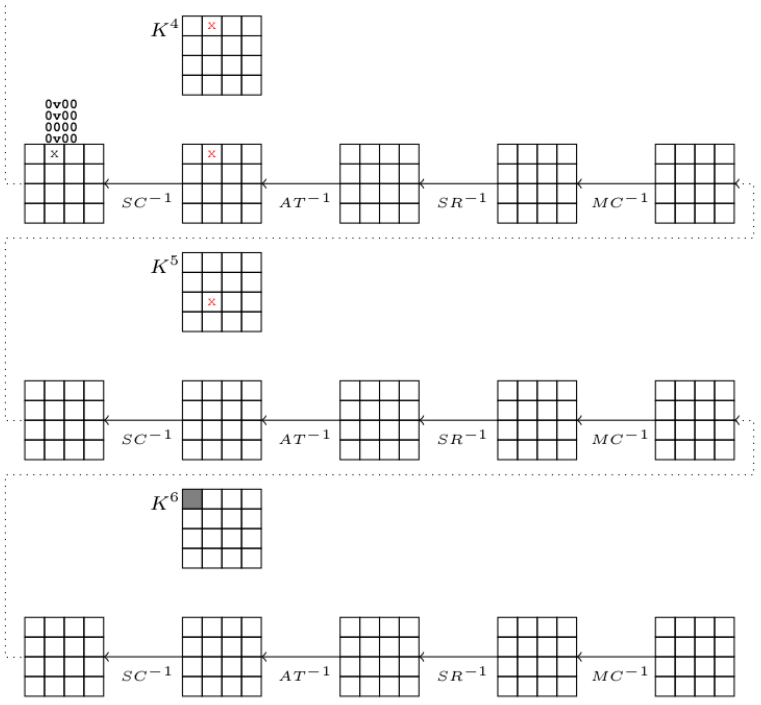
- Extend trail by 6 rounds in backward and 4 rounds in forward direction
- Related-Tweakey attack, as we insert a difference in position 11 of the Tweakey
- The inserted difference is in a specific form, so that after 6 rounds the Tweakey difference is 0

$$
\begin{aligned}
k^6[0] + \overline{k^6}[0] &= tk_1^6[0] + \overline{tk_1^6}[0] + tk_2^6[0] + \overline{tk_2^6}[0] \\
&= tk_1^1[11] + \overline{tk_1^1}[11] + L^3\left(tk_2^1[11]\right) + L^3\left(\overline{tk_2^1}[11]\right) \\
&= \delta_1 + L^3\left(\delta_2\right) = 0
\end{aligned}
$$

where $\delta_1 = tk_1^1[11] + \overline{tk_1^1}[11]$ and $\delta_2 = tk_2^1[11] + \overline{tk_2^1}[11]$

Key Recovery - backward rounds





Key Recovery - backward rounds

1. Take any plaintext P and calculate after the first round MixColumn
2. Choose difference α in E^2 in cell position 14
3. The attacker calculates then $k^1[1]$, $k^1[3]$, $k^1[7]$ so that

$$B^2 \oplus \overline{B^2} = \mathrm{Lin}^{-1}(E^2) \oplus \mathrm{Lin}^{-1}(\overline{E^2}) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & \beta \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha \end{bmatrix}.$$

   For example, $k^1[1]$ is a solution of the equation:

$$S\left(E^1[5] \oplus k^1[1]\right) \oplus S\left(E^1[5] \oplus \Delta_1 \oplus k^1[1]\right) = \alpha.$$

   Note that according to Lemma 1, the equation above has one solution on average.
4. The attacker can now recover $\overline{P}$ by inverting MC, SR, AC and SC on $\overline{E^1}$

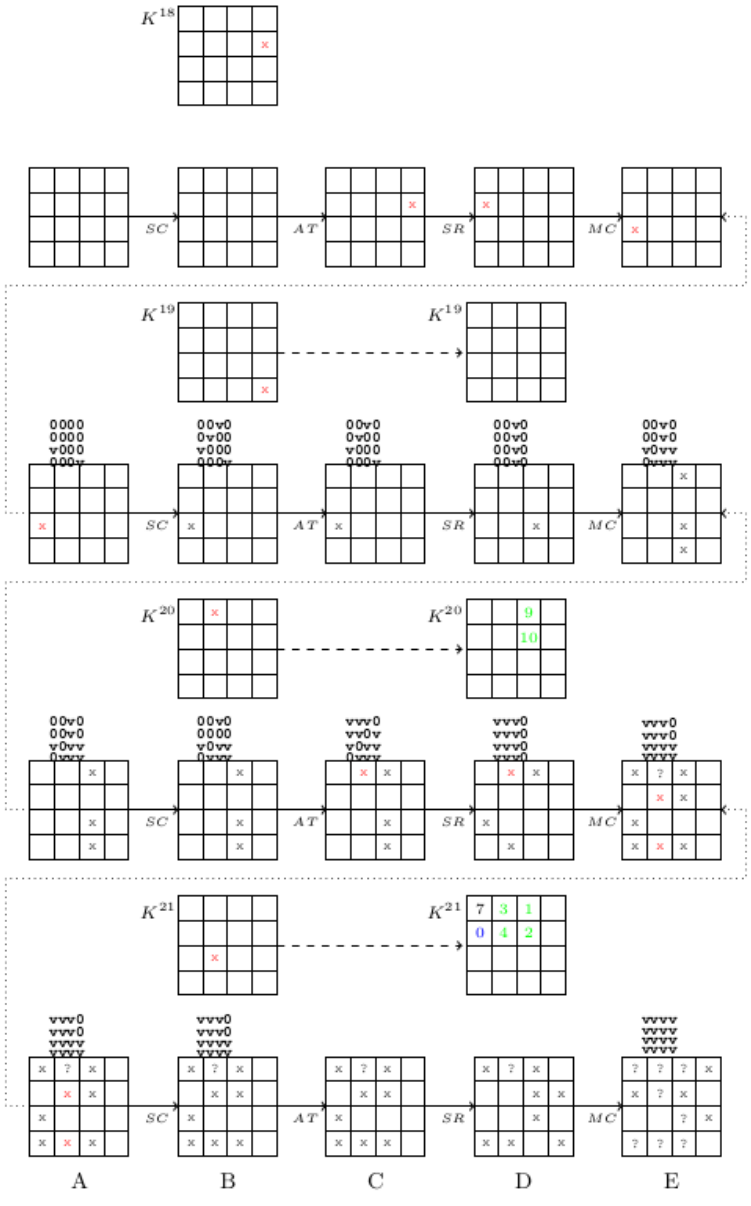
Key Recovery - backward rounds

5. The attacker still needs to cancel the active nibble in $B^4[1]$ with $\delta_1 \oplus L^2(\delta_2)$
6. Therefore the attacker needs to guess three additional key values in Round 1 (*i.e.* $k^1[2]$, $k^1[4]$, $k^1[6]$) and three additional key values in Round 2 (*i.e.* $k^2[1] = tk_1^1[15] + L(tk_2^1[15])$, $k^2[2] = tk_1^1[8] + L(tk_2^1[8])$, $k^2[6] = tk_1^1[12] + L(tk_2^1[12]))$
7. Guessing the tweakey nibbles mentioned above enables the attacker to calculate the value of $B^3[1]$. Then, she calculates $k^3[1] = tk_1^1[7] \oplus L(tk_2^1[7])$ as follows. Since $D^3[1] = B^3[1] \oplus k^3[1]$ holds, we have:

$$S\left(D^3[1] \oplus D^3[9] \oplus D^3[13]\right) \oplus S\left(D^3[1] \oplus D^3[9] \oplus \overline{D^3}[13]\right) = \delta_1 \oplus L^2(\delta_2).$$

8. There are no active nibbles after round 4
9. The tweakey difference in round 5 is not added
10. $\delta_1 + L^3(\delta_2) = 0$ cancels the tweakey difference in round 6

Key Recovery - forward rounds



Key Recovery - forward rounds

1. The attacker rejects ciphertext pairs which do not have seven inactive cells in cells (3, 4, 5, 8, 9, 11, and 14) after peeling off the final MixColumns layer. Thus, a fraction of 2^{-28} pairs are filtered.
2. The attacker rejects ciphertext pairs which do not have the difference $\delta_1 \oplus L^{10}(\delta_2)$ in cell 13 of A^{21}.
3. The attacker determines $k^{21}[5] = tk_1^1[4] \oplus L^{10}(tk_2^1[4])$ so that the active nibble in cell 5 of A^{21} is $\delta_1 \oplus L^{10}(\delta_2)$. The attacker determines $k^{21}[2] = tk_1^1[1] \oplus L^{10}(tk_2^1[1])$ and $k^{21}[6] = tk_1^1[2] \oplus L^{10}(tk_2^1[2])$ so that the active nibble in cell 2 and 6 of A^{21} are equal to the active nibble in cell 14. Additionally, the attacker guesses $k^{21}[4] = tk_1^1[0] \oplus L^{10}(tk_2^1[0])$.

Key Recovery - forward rounds

4. The attacker can then calculate:

$$A^{20}[10] \oplus \overline{A^{20}}[10] = S^{-1}\left(B^{20}[10]\right) \oplus S^{-1}\left(\overline{B^{20}}[10]\right)$$
$$= S^{-1}\left(D^{20}[8]\right) \oplus S^{-1}\left(\overline{D^{20}}[8]\right) = \eta.$$

$$A^{20}[14] \oplus \overline{A^{20}}[14] = S^{-1}\left(D^{20}[13]\right) \oplus S^{-1}\left(\overline{D^{20}}[13]\right)$$
$$= S^{-1}\left(A^{21}[1] \oplus A^{21}[13]\right) \oplus S^{-1}\left(\overline{A^{21}}[1] \oplus \overline{A^{21}}[13]\right).$$

5. The attacker calculates $k^{20}[2] = tk_1^1[9] \oplus L^{10}(tk_2^1[9])$ and can then calculate:

$$\eta = A^{20}[2] \oplus \overline{A^{20}}[2] = S^{-1}\left(C^{20}[2] \oplus k^{20}[2]\right) \oplus S^{-1}\left(\overline{C^{20}}[2] \oplus k^{20}[2]\right).$$

6. The final condition to be satisfied is that the active nibble in cell 8 of A^{19} has to be equal to $\delta_1 \oplus L^9(\delta_2) = \gamma$.

Attack Algorithm

1. Choose a random plaintext P and request the corresponding ciphertext C
2. Choose differences δ_1 and δ_2 such that $\delta_1 = L^3(\delta_2)$.
3. Calculate backwards rounds to get $\overline{P}$
4. Request ciphertext $\overline{C}$
5. Calculate forward rounds/do filtering

Repeat above procedure for 2^x plaintexts until a single key solution remains.

Time complexity = 2^{86}

Extension to 22/23 rounds

Extension to 22 rounds

- Assume that 48 bits of the 128bit tweakey are public tweak, 80 bits for the secret key
- Select the following cell positions for the tweak TK[i] for i = 8,11,12,13,14,15
- We can add a round in the end
- We slightly have to change the attack procedure, as we do not have to guess *tweak* bits
- Time complexity = $2^{71.6}$

Extension to 23 rounds

- We can prepend a round in the beginning
- We only have to guess 2 more tweakey nibbles
- Time complexity = 2^{79}

Conclusion

- We showed a Related-Tweakey Impossible-Differential Attack on up to 21 rounds of SKINNY
- We can extend it to 23 rounds under the assumption of having 48 bits public tweak and 80 bits secret key
- SKINNY remains secure, with still 13 rounds security margin
- Additional 3rd party security analysis is needed!

Questions?

Thank you for your attention!

Related-Key Impossible-Differential Attack on Reduced-Round SKINNY
http://eprint.iacr.org/2016/1127

References I

Eli Biham, Alex Biryukov, and Adi Shamir.
Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials.
In Jacques Stern, editor, *EUROCRYPT*, volume 1592 of *Lecture Notes in Computer Science*, pages 12–23. Springer, 1999.

Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim.
Cryptanalysis competition.
`https://sites.google.com/site/skinnycipher/cryptanalysis-competition`, 2016.

References II

Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim.
The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers.
The SIMON and SPECK Families of Lightweight Block Ciphers.
Cryptology ePrint Archive, Report 2013/404, 2013.
`http://eprint.iacr.org/`.

Jérémy Jean, Ivica Nikolic, and Thomas Peyrin.
Tweaks and Keys for Block Ciphers: The TWEAKEY Framework.
In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT (2)*, volume 8874 of *Lecture Notes in Computer Science*, pages 274–288, 2014.

References III


Lars Knudsen.
DEAL - A 128-bit Block Cipher.
In *NIST AES Proposal*, 1998.


Guozhen Liu, Mohona Ghosh, and Song Ling.
Security Analysis of SKINNY under Related-Tweakey Settings.
Cryptology ePrint Archive, Report 2016/1108, 2016.
http://eprint.iacr.org/2016/1108.


Sadegh Sadeghi, Tahere Mohammadi, and Nasour Bagheri.
Cryptanalysis of Reduced round SKINNY Block Cipher.
Cryptology ePrint Archive, Report 2016/1120, 2016.
http://eprint.iacr.org/2016/1120.


Mohamed Tolba, Ahmed Abdelkhalek, and Amr M. Youssef.
Impossible Differential Cryptanalysis of Reduced-Round SKINNY.
Cryptology ePrint Archive, Report 2016/1115, 2016.
http://eprint.iacr.org/2016/1115.