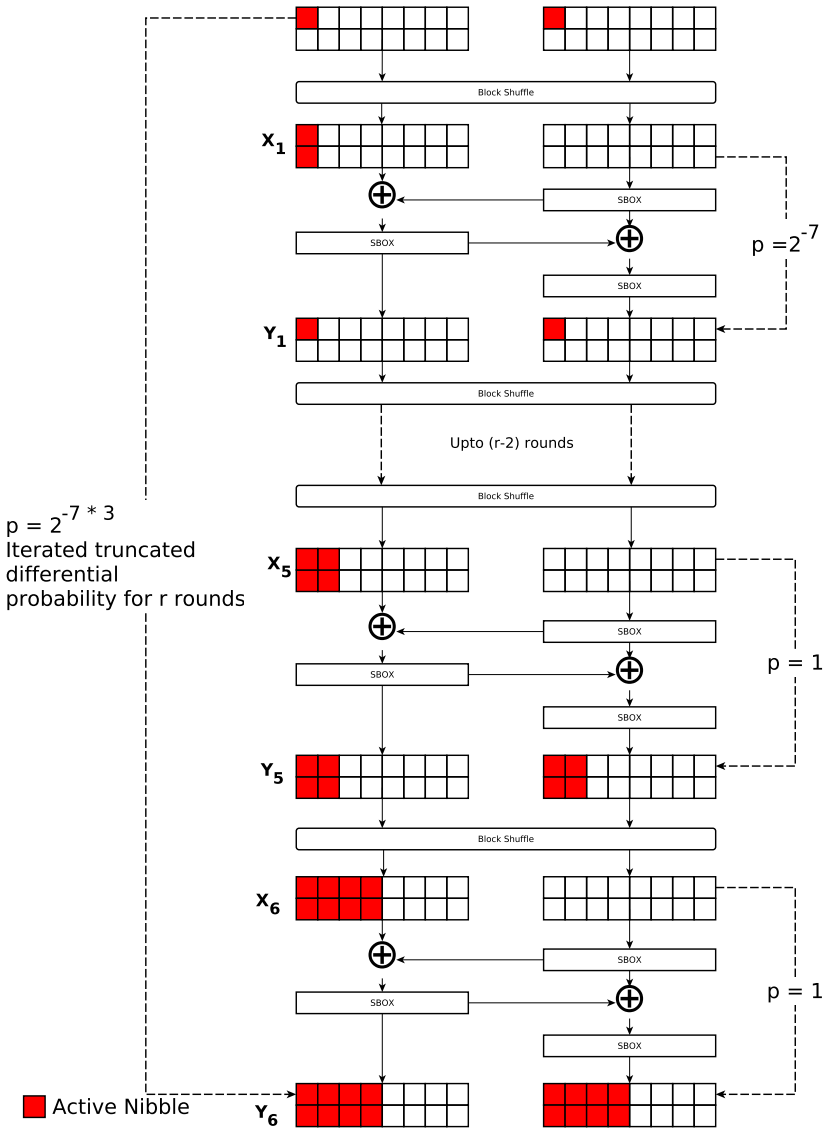
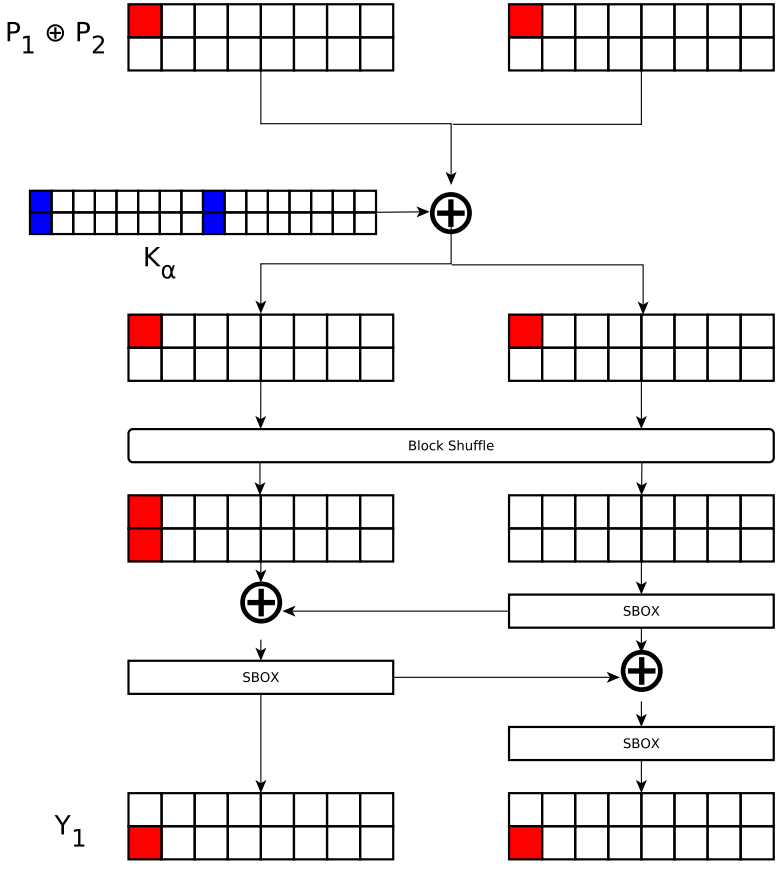
Iterated Truncated Differential: Distinguisher



- Number of free rounds is 3
- Probability of 6-round FLEX-128 distinguisher is 2^{-7*3}
- In similar way, number of free rounds in 5-round FLEX-64 and 7-round FLEX-256 is 2 and 4 respectively

Iterated Truncated Differential: Key Recovery



- Find a right pair (P_1, P_2), such that difference is in byte 0 and 8
- Guess Key byte 0 and 8 (2^{16} possible guesses)
- Run one round encryption and check whether same of byte 0 and 8 are active or not in Y_1 (2^9 key candidates remain)
- Use two more right pairs to reduce key candidates to 1
- Repeat the procedure for 8 more byte pairs

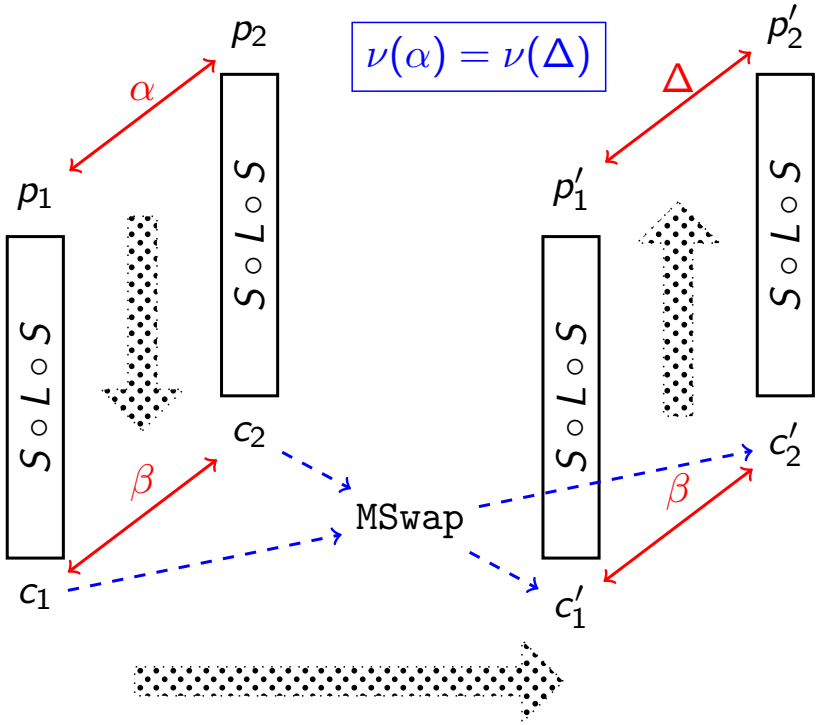
Iterated Truncated Differential Attacks: Summary

Block Size	#rounds	Data Complexity		Time Complexity	Memory Complexity
		Encs	Decs	MAs	
64	7	$2^{30.5}$		$2^{34.5}$	$2^{18.5}$
128	16	$2^{93.5}$		$2^{108.5}$	$2^{20.5}$
256	21	$2^{109.5}$		$2^{125.5}$	$2^{22.5}$

Yoyo Attacks

$G_2' = L \circ S \circ L \circ S$ Two full generic Rounds

$G_2 = S \circ L \circ S$ ← Dropping final linear layer (to simplify)



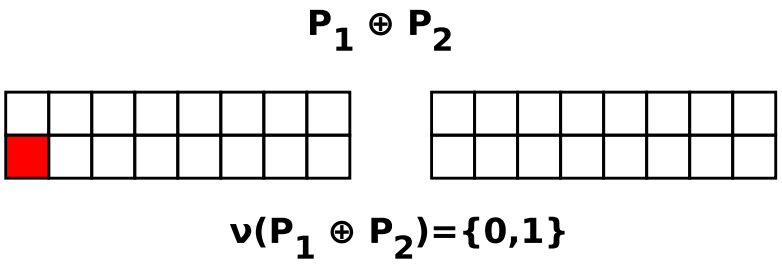
- ν is the Zero Difference Pattern

Applied to AES

- First key-independent Yoyo distinguishers of AES
- 5-round Key Recovery

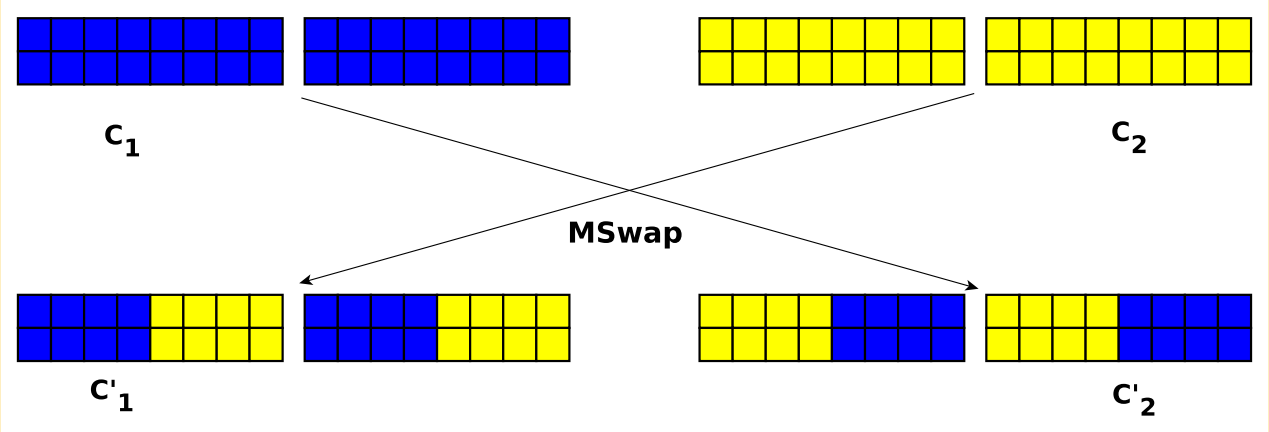
The Yoyo Trick

Zero Difference Pattern



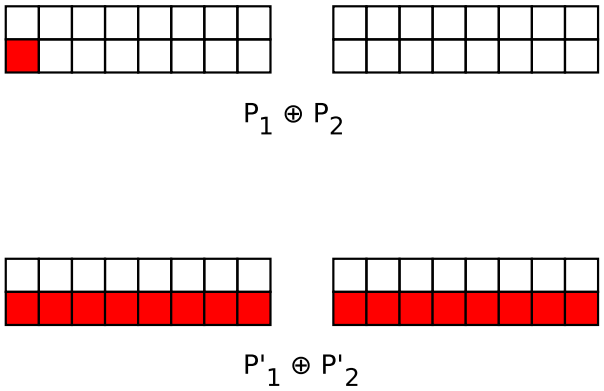
- Two Super-Sbox in FLEX-128 state
- A fully inactive Super-Sbox is denoted by 1; otherwise, 0

MSwap



- Bytes are swapped between two texts according Super-Sbox output

Yoyo Attacks: Deterministic Distinguisher

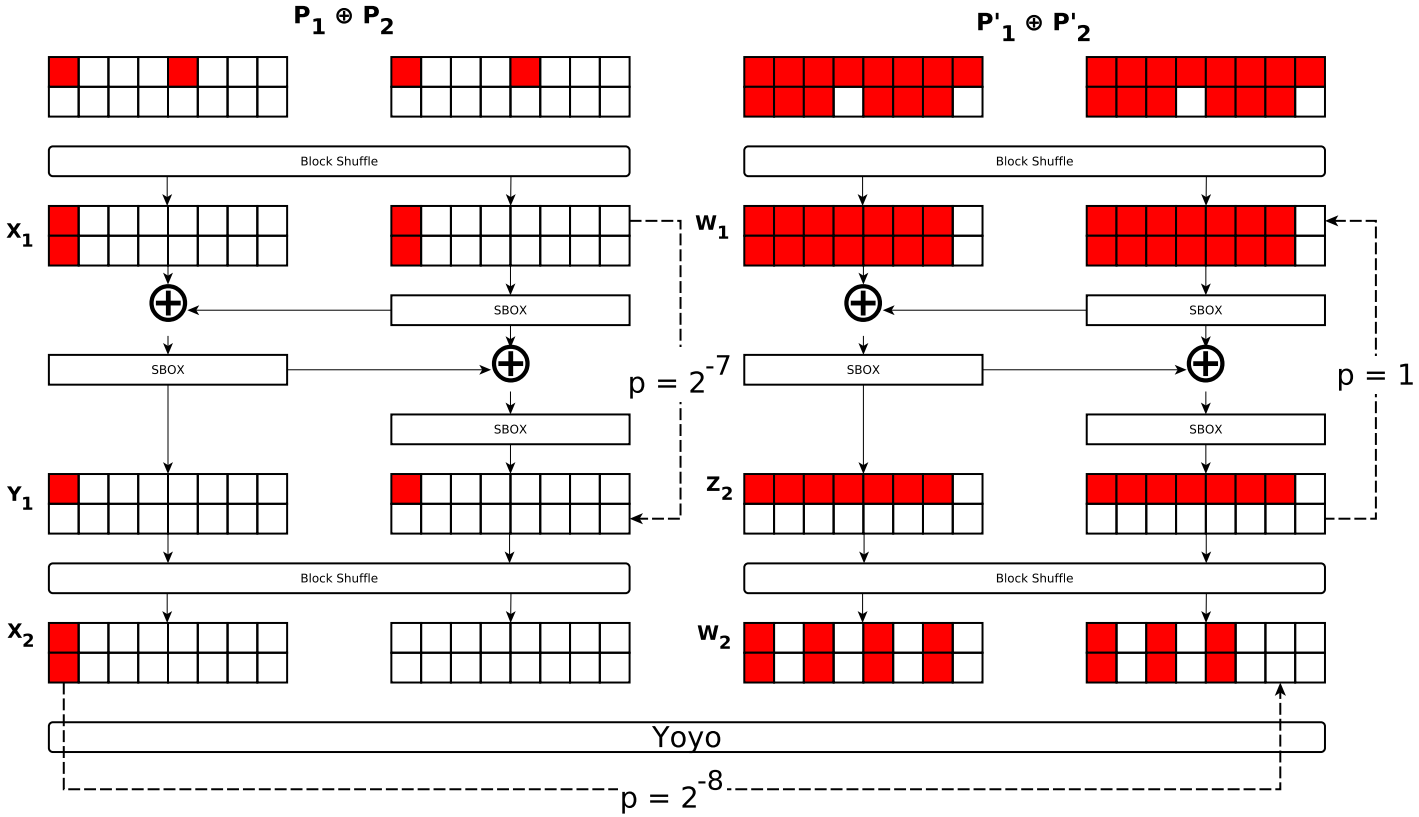


- Super-Sbox and `BlockShuffle` are considered as S and L layer respectively
- FLEX-128 Super-Sbox spans over 2.5 rounds
- 6-round FLEX-128 Deterministic Distinguisher
- Apply Yoyo game
  1. $P_1, P_2 \xrightarrow{ENC} C_1, C_2$
  2. $C_1, C_2 \xrightarrow{MSwap} C_1', C_2'$
  3. $C_1', C_2' \xrightarrow{DEC} P_1', P_2'$

Yoyo Attacks: Key Recovery

- 6-round Deterministic Distinguisher is the building block of 7-round FLEX-128 Key Recovery attack
- Byte to Nibble Transition is used to extend for 1 round
- Similar kinds of attacks exist for FLEX-64 and FLEX-256

Yoyo Attacks: Key Recovery



- Choose P_1, P_2 and encrypt them to obtain C_1, C_2
- Apply *MSwap* on C_1, C_2 and decrypt them to get P_1', P_2'
- Any one of the 8 active Bytes in W_2 can be zero w.p. 2^{-5}
- Trail probability is 2^{-12}
- Key Recovery part is same as Iterated Truncated Differential

Yoyo Attacks: Summary

Block Size	#rounds	Data Complexity		Time Complexity	Memory Complexity
		Encs	Decs	MAs	
64	5	2^{10}	$2^{16.5}$	$2^{15.5}$	2^{10}
128	7	$2^{10.5}$	$2^{16.5}$	$2^{16.5}$	$2^{11.5}$
256	9	2^{11}	$2^{16.5}$	$2^{17.5}$	2^{13}

Attacks Presented in this Work

Block Size	#rounds	Data Complexity		Time Complexity	Memory Complexity	Attack Type
		Encs	Decs	MAs		
64	7	$2^{30.5}$		$2^{34.5}$	$2^{18.5}$	Iterated Truncated Differential
	5	2^{10}	$2^{16.5}$	$2^{15.5}$	2^{10}	Yoyo Attack
128	16	$2^{93.5}$		$2^{108.5}$	$2^{20.5}$	Iterated Truncated Differential
	7	$2^{10.5}$	$2^{16.5}$	$2^{16.5}$	$2^{11.5}$	Yoyo Attack
256	21	$2^{109.5}$		$2^{125.5}$	$2^{22.5}$	Iterated Truncated Differential
	9	2^{11}	$2^{16.5}$	$2^{17.5}$	2^{13}	Yoyo Attack

Conclusion

1. Reported Iterated Truncated Differential which exploits AES Sbox and `BlockShuffle` operation
2. Generalized Yoyo Distinguishing Attack is applicable
3. All attacks are exploited to recover subkeys
4. Practical ones are experimentally verified
5. FlexAEAD is out of 2nd round

Thank You