Meet-in-the-Middle Attacks on Classes of Contracting and Expanding Feistel Constructions

Jian Guo Jérémy Jean Ivica Nikolić Yu Sasaki

FSE 2017 @ Tokyo, Japan
06 March 2017

Outline

Development of MITM Attacks

Two independent functions:

- Diffe & Hellman'77
- Application to Double-DES [Chaum-Evertse'85]
- Many applications to block ciphers ...
- Application to preimages of hash functions [Sasaki et al'08]
- Application to collisions of hash functions [Li et al'12]
- Back to block ciphers, KTANTAN, XTEA, etc.

Development of MITM Attacks

Two independent functions:

- Diffe & Hellman'77
- Application to Double-DES [Chaum-Evertse'85]
- Many applications to block ciphers ...
- Application to preimages of hash functions [Sasaki et al'08]
- Application to collisions of hash functions [Li et al'12]
- Back to block ciphers, KTANTAN, XTEA, etc.

Function Matching:

- Collision attack on Rijndael [Gilbert-Minier'00]
- MITM attack on AES [Demirci-Selcuk'08]
- Improved attack on AES [Dunkelman et al'10]
- Improved attack on AES [Derbez et al'13]
- Improved attack on Feistel [Ours'14]

Development of MITM Attacks

Two independent functions:

- Diffe & Hellman'77
- Application to Double-DES [Chaum-Evertse'85]
- Many applications to block ciphers ...
- Application to preimages of hash functions [Sasaki et al'08]
- Application to collisions of hash functions [Li et al'12]
- Back to block ciphers, KTANTAN, XTEA, etc.

Function Matching:

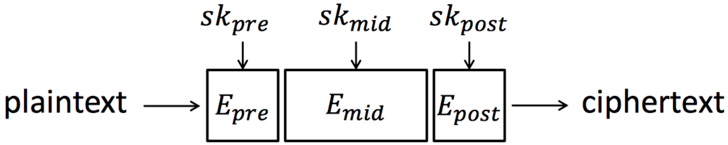
- Collision attack on Rijndael [Gilbert-Minier'00]
- MITM attack on AES [Demirci-Selcuk'08]
- Improved attack on AES [Dunkelman et al'10]
- Improved attack on AES [Derbez et al'13]
- Improved attack on Feistel [Ours'14]
- Attack on Contracting and Expanding Feistels [**This Talk**]

The Core of MITM Attacks

Find n-bit collision of two functions in $2^{n/2}$, due to birthday paradox

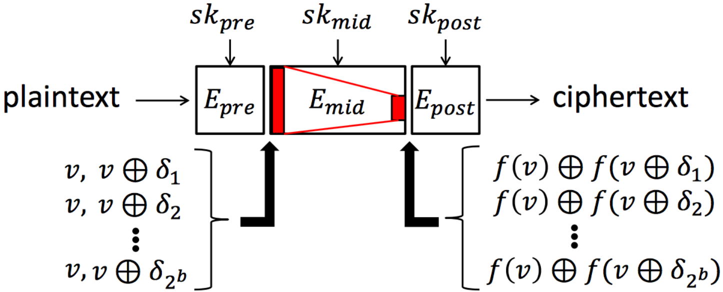
- Useful when the ideal security level is more than $2^{n/2}$, e.g., (second-) preimage of hash functions
- When attacking a single function, split it into two independent sub-functions

Function Match - Overview 1/2



- Used for key recovery, divide the cipher into three parts: $E = E_{pre} \circ E_{mid} \circ E_{post}$
- E_{pre} and E_{post} are handled by bruteforcely guessing sk_{pre} and sk_{post}.
- sk_{mid} is recovered by **function match**, i.e., each key from sk_{mid} corresponds to an E_{mid}

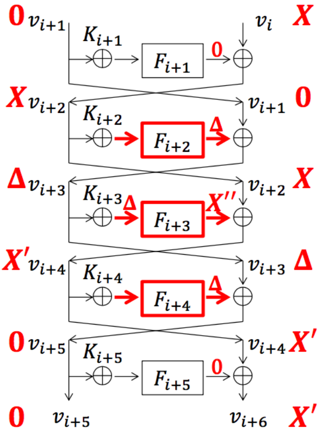
Function Match - Overview 2/2



- build the link between E_{mid} and **b-δ-set**.
- offine: store the set $f(v) \oplus f(v \oplus \delta_j)$ for $j = 1, \ldots 2^b$ in lookup table T_δ.
- online: compute the b-δ-set, and recover the corresponding key from T_δ.

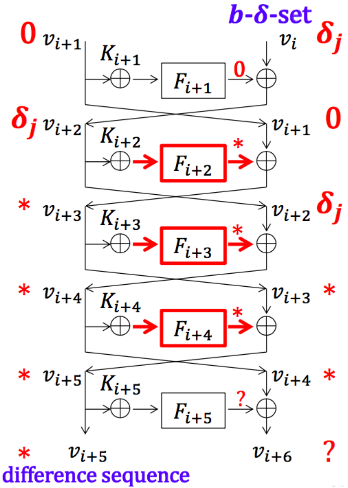
Application to Feistel-2: Distinguisher

- Fix the difference X and X' with $X \neq X'$
- The number of possibility of internal values is $2^{n/2}$ v.s. $2^{3n/2}$, once Δ is fixed, all internal values of middle 3 rounds are fixed.



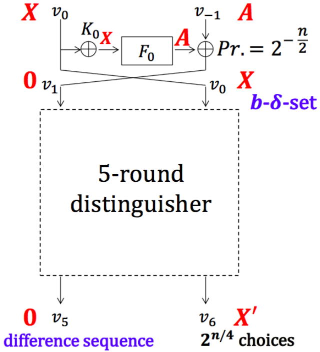
Application to Feistel-2: b-δ-set

- Once a pair of message $(v, v \oplus (0\|X))$ with output difference $(0, X')$ is conformed
- find the output difference of the left branch of any message $(v, v \oplus (0\|\delta_j))$



Applications to Feistel-2: Key Recovery

1. Randomly choose a v_0
2. Query all $(v_0, *)$ and $(v_0 \oplus X, *)$ to obtain 2^n pairs
3. $2^{n/4}$ pairs will be in the set of $(0, X')$ of size $2^{n/4}$.
4. Iterate above $2^{n/4}$ times by varying v_0. $2^{n/2}$ good output pairs obtained.
5. For each pair, recover input value to F_0, i.e., $v_0 \oplus K_0$, hence K_0
6. With the recovered K_0, prepare b-δ-set at v_0, compute the corresponding v_{-1}, obtain the sequence of Δv_5 and check against the precomputed T_δ. Check correctness of the guessed K_0.



Overall Complexity: $2^{3n/4}$ for time, data, memory.

Key Factors Deciding #Rounds Attacked

#Rounds for Distinguisher

What is the maximum number of rounds of the cipher s.t. #functions $< 2^k$?

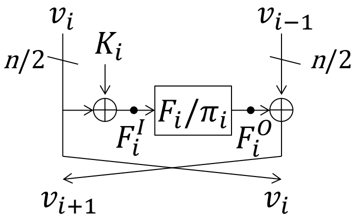
#Rounds for E_{pre} and E_{post}

What is the maximum number of rounds that can be added before and after the distinguisher?

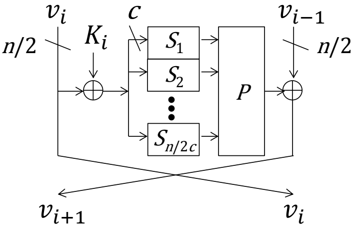
Results of Generic Feistel [Guo-Jean-Nikolić-Sasaki AC'14]

#Rounds Attacked

Type	Key Size		
	n	$3n/2$	$2n$
Feistel-2	6	8	10
Feistel-3	9	11	13
Feistel-3 (identical)	10	12	14



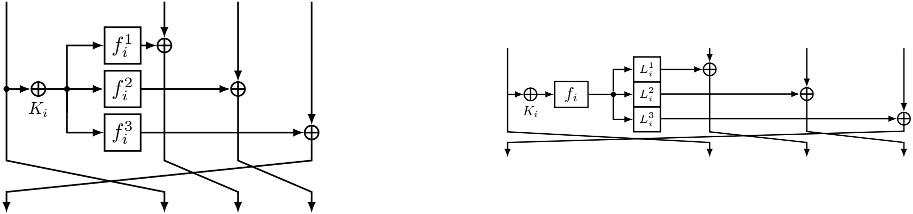
Feistel-2



Feistel-3

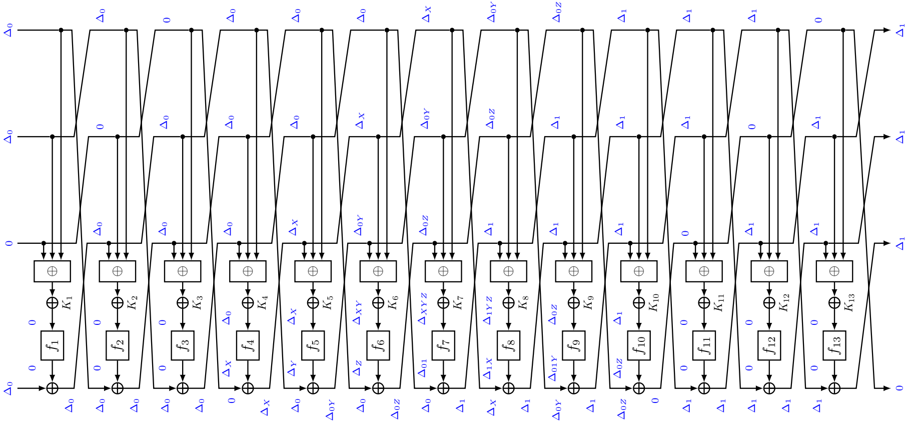
This Work - More Specific Functions

Contracting Feistel



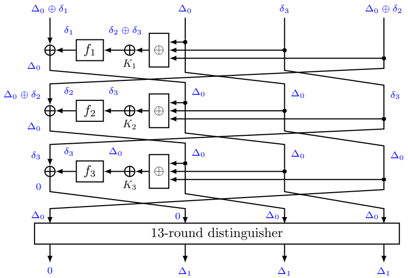
Expanding Feistel

Contracting Feistel: 13R Distinguisher



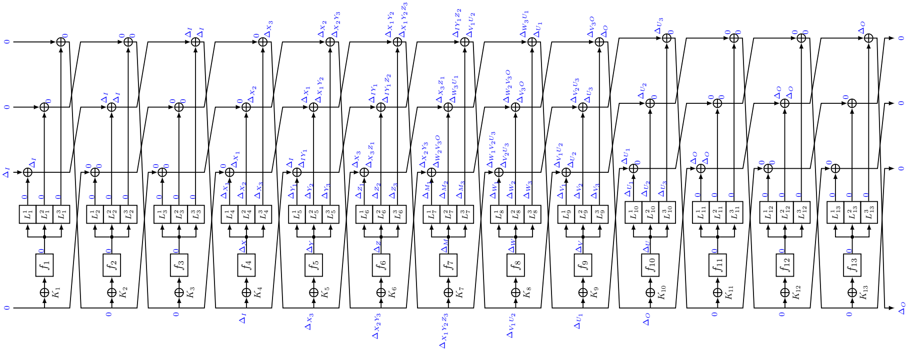
There are $2^{3n/4}$ possibilities.

Contracting Feistel: 16R Key Recovery



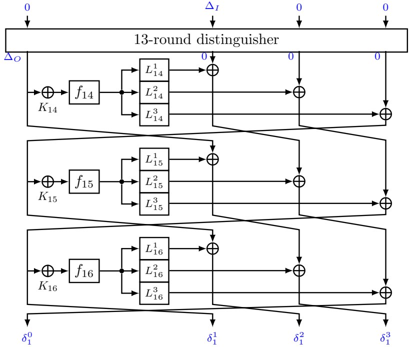
- $|sk_{pre}| = 2^{3n/4}$ and $|sk_{post}| = 2^0$
- Online/Offline: $2^{7n/8}$ time, memory, data

Expanding Feistel-FL: 13R Distinguisher



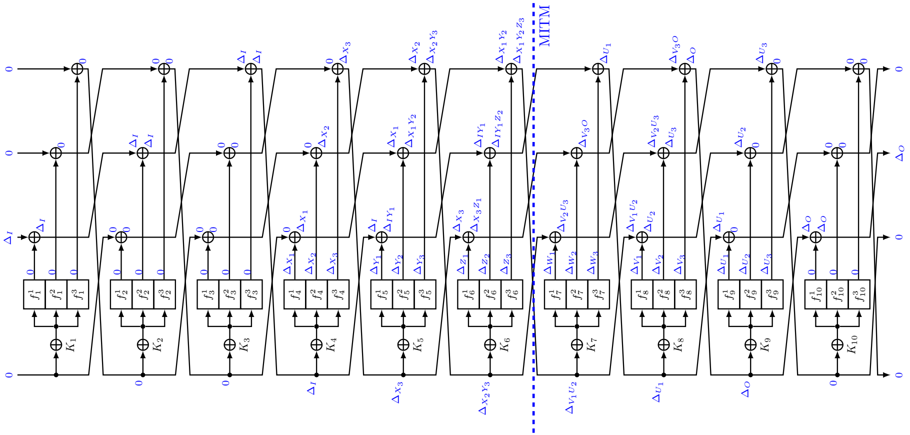
There are $2^{3n/4}$ possibilities.

Expanding Feistel-FL: 16R Key Recovery



- $|sk_{pre}| = 2^0$ and $|sk_{post}| = 2^{3n/4}$
- Online/Offline: $2^{7n/8}$ time, memory, data

Expanding Feistel: 10R Distinguisher



Distinguisher for 10 rounds, and attack for 13 rounds.

Result Summary

Type	Bit Length of Key k (d branches)	#rounds	
		Patarin et al.	Ours
Contracting Feistel (Section 3)	n	$2d-1$	$5d-4$
	$2n$	$2d-1$	$7d-4$
	$n+\frac{rn}{d}$	$2d-1$	$5d-4+2r$
Expanding Feistel-F (Section 4)	n	$3d-1$	$4d-3$
	$n+\frac{n}{d}$	$3d-1$	$4d$
	$2n$	$3d-1$	$6d-3$
	$n+\frac{rn}{d}$	$3d-1$	$4d-3+2r$ †
Expanding Feistel-FL (Section 5)	n	$3d-1$	$5d-4$
	$2n$	$3d-1$	$7d-4$
	$n+\frac{rn}{d}$	$3d-1$	$5d-4+2r$

End of Presentation

Thanks for your attention !

Question ?