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

1. Introduction to MITM Attacks

2. Applications to Feistel [Guo-Jean-Nikolic-Sasaki AC’14]

3. Application to Contracting and Expanding Feistels

4. Conclusions
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 bruteforce guessing \( sk_{pre} \) and \( sk_{post} \).
- \( sk_{mid} \) is recovered by function match, i.e., each key from \( sk_{mid} \) corresponds to an \( E_{mid} \).
build the link between $E_{\text{mid}}$ and $b$-$\delta$-set.

- offline: store the set $f(v) \oplus f(v \oplus \delta_j)$ for $j = 1, \ldots 2^b$ in lookup table $T_{\delta}$.
- online: compute the $b$-$\delta$-set, and recover the corresponding key from $T_{\delta}$.
- 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 $\Delta$ is fixed, all internal values of middle 3 rounds are fixed.
Application to Feistel-2: $b$-$\delta$-set

- Once a pair of message $(\nu, \nu \oplus (0\|X))$ with output difference $(0, X')$ is conformed
- find the output difference of the left branch of any message $(\nu, \nu \oplus (0\|\delta_j))$
Applications to Feistel-2: Key Recovery

1. Randomly choose a $v_0$

2. Query all $(v_0, \ast)$ and $(v_0 \oplus X, \ast)$ 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 $b$-$\delta$-set at $v_0$, compute the corresponding $v_{-1}$, obtain the sequence of $\Delta v_5$ and check against the precomputed $T_\delta$. 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 \(E_{\text{pre}}\) and \(E_{\text{post}}\)

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]

<table>
<thead>
<tr>
<th>Type</th>
<th>Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$n$</td>
</tr>
<tr>
<td></td>
<td>$3n/2$</td>
</tr>
<tr>
<td></td>
<td>$2n$</td>
</tr>
<tr>
<td>Feistel-2</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>10</td>
</tr>
<tr>
<td>Feistel-3</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>13</td>
</tr>
<tr>
<td>(identical)</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>14</td>
</tr>
</tbody>
</table>

**Guo, Jean, Nikolić, Sasaki**

**MITM Attacks on Feistels**

**FSE 2017**
This Work - More Specific Functions

Contracting Feistel

Expanding Feistel
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

13-round distinguisher

- $|sk_{pre}| = 2^0$ 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

<table>
<thead>
<tr>
<th>Type</th>
<th>Bit Length of Key $k$</th>
<th>#rounds</th>
<th>Patarin et al.</th>
<th>Ours</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(d branches)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contracting</td>
<td>$n$</td>
<td>$2d - 1$</td>
<td>$5d - 4$</td>
<td></td>
</tr>
<tr>
<td>Feistel</td>
<td>$2n$</td>
<td>$2d - 1$</td>
<td></td>
<td>$7d - 4$</td>
</tr>
<tr>
<td>(Section 3)</td>
<td>$n + \frac{rn}{d}$</td>
<td>$2d - 1$</td>
<td></td>
<td>$5d - 4 + 2r$</td>
</tr>
<tr>
<td>Expanding</td>
<td>$n$</td>
<td>$3d - 1$</td>
<td>$4d - 3$</td>
<td></td>
</tr>
<tr>
<td>Feistel-F</td>
<td>$n + \frac{n}{d}$</td>
<td>$3d - 1$</td>
<td></td>
<td>$4d$</td>
</tr>
<tr>
<td>(Section 4)</td>
<td>$2n$</td>
<td>$3d - 1$</td>
<td></td>
<td>$6d - 3$</td>
</tr>
<tr>
<td></td>
<td>$n + \frac{rn}{d}$</td>
<td>$3d - 1$</td>
<td></td>
<td>$4d - 3 + 2r \dagger$</td>
</tr>
<tr>
<td>Expanding</td>
<td>$n$</td>
<td>$3d - 1$</td>
<td>$5d - 4$</td>
<td></td>
</tr>
<tr>
<td>Feistel-FL</td>
<td>$2n$</td>
<td>$3d - 1$</td>
<td></td>
<td>$7d - 4$</td>
</tr>
<tr>
<td>(Section 5)</td>
<td>$n + \frac{rn}{d}$</td>
<td>$3d - 1$</td>
<td></td>
<td>$5d - 4 + 2r$</td>
</tr>
</tbody>
</table>
End of Presentation

Thanks for your attention!

Question?