Analysis of FOX

Jorge Nakahara Jr
jorge_nakahara@yahoo.com.br

Presented by: Mads Rasmussen
mads@lsitec.org.br

Summary

- The FOX block cipher family
- Information leakage in FOX
- Impossible-Differential Analysis
- Conclusions

The FOX Cipher Family

- **Designers: P. Junod and S. Vaudenay (2004)**
- **New name: IDEA-NXT**
- **Owned by Mediacrypt A.G.**
- **Lai-Massey structure, like IDEA cipher**
- **Two main ciphers: FOX64 and FOX128**
- **Byte-oriented design: byte are elements of GF(2^8) = GF(2)[x]/(x^8+x^7+x^6+x^5+x^4 +x^3+1)**

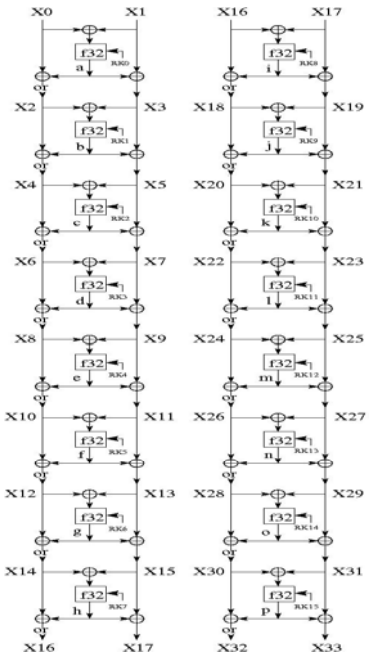
The FOX Cipher Family

- Each round of FOX64 uses a bijective mapping called f32 consisting of an MDS matrix, xor with two round subkeys, and an 8x8-bit S-box
- Each round of FOX128 uses a bijective mapping called f64, consisting of an MDS matrix, xor with two round subkeys and an 8x8-bit S-box
- To break the round symmetry, there is a linear transformation called orthomorphism (**or**) at the end of each round.

The FOX Cipher Family

Cipher	Block Size (bits)	Key Size (bits)	#rounds
FOX64	64	128	16
FOX128	128	256	16
FOX64/k/r	64	k ($0 \le k \le 256$)	r ($12 \le r \le 255$)
FOX128/k/r	128	k ($0 \le k \le 256$)	r ($12 \le r \le 255$)

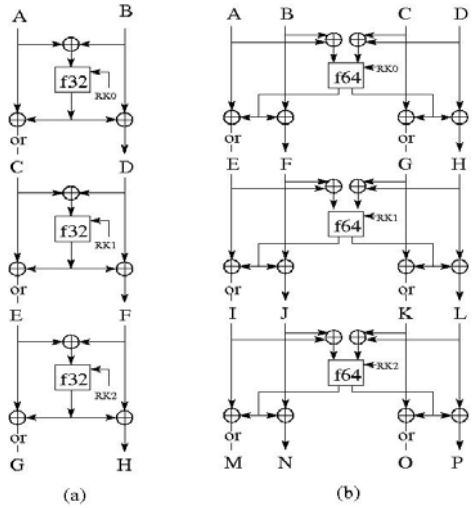
FOX64



Information Leakage

- **Information leakage: discover (non-trivial) internal cipher data using only (known) plaintext-ciphertext pairs.**
- **More especifically, for FOX, use the high level Lai-Massey scheme.**
- **Such kind of leakage absent in IDEA cipher.**
- **Leakage leads to full break of FOX64/k/2 and FOX128/k/2.**

3-round FOX64 and FOX128



SBSeg 2008, Gramado, RS, Brazil

Information Leakage

- Consider 2-round FOX64, for ex., the top 2 rounds of the previous slide.
- From the Lai-Massey scheme:
  $A \oplus B = io(C) \oplus D$, $C \oplus D = io(E) \oplus F$, where $\oplus$ is exclusivo-or and **io** is the inverse of **or**.
- Known-plaintext (KP) setting.
- Thus, $D \oplus or(D) = or(A \oplus B) \oplus io(E) \oplus F$
  and $C \oplus io(C) = A \oplus B \oplus io(E) \oplus F$, and
  both C and D can be uniquely determined.

Information Leakage

- But C and D are internal cipher values !!
- Thus, we have discovered the input and output values of both f32 mappings of 2-round FOX64
- Consequently, we can attack each f32 mapping separately, and discover the round subkey of each f32 in turn.
- Conclusion: we can break 2-round FOX64

Information Leakage

- A similar reasoning applies to FOX128/k/2.
- Analogously, a similar approach holds to more than 2 rounds. But, rather than individual 32-bit values, we obtain an xor of 32-bit internal data.
- A similar kind of leakage was already observed in DES (due to D.W.Davies and S. Murphy), due to the Feistel structure.

Impossible-Differential Technique

- Developed by L.R.Knudsen and first applied on DEAL block cipher (1998)
- Biham also mentions its use (implicitly) in Enigma machine
- Impossible Diff. (ID) technique uses tools from differential cryptanalysis (DC)
- Unlike DC, though, ID uses differentials with probability zero (never hold)

Impossible-Differential Technique

- ID distinguishers consist of two (truncated) differentials, called Δ and ▼, both of which hold with certainty.
- ▼ propagates differences in the encryption direction; Δ propagates differences in the decryption direction.
- The combination of Δ and ▼ makes up the ID distinguisher: $▼ \not\rightarrow Δ$ and $▼ \not\leftarrow Δ$.
- That is the reason for the name “impossible differential”.

Impossible-Differential Technique

- For FOX64, we have found a 3-round ID distinguisher.
- In particular, we have found that

  $(Δ,Δ,Δ,Δ) \not\rightarrow (Δ,Δ,0,Δ)$

  where each Δ stands for a 32-bit nonzero xor difference.
- This fact by itself already allows one to distinguish 3-round FOX64 from a random permutation. But further, we can recover subkeys around this distinguisher.

Impossible-Differential Technique

- Attack complexities:
  time: 2^{118} 5-round FOX64 computations
  data: 2^{36} CP
  memory: 2^{122} text blocks

  time: 2^{198} 6-round FOX128 computations
  data: 2^{52} CP
  memory: 2^{249} text blocks
  See attack details in the paper, please.

Conclusions and Open Problems

- This paper presented some cryptanalytic results of reduced-round FOX ciphers, such as information leakage and impossible differential attacks.
- The attacks do not threaten any official version of FOX (with the suggested parameters), but show new avenues for attacks.

Questions???

Send your doubts to

jorge_nakahara@yahoo.com.br