Complementing Feistel Ciphers

Ivica Nikolić (joint work with Alex Biryukov)

Nanyang Technological University, Singapore
University of Luxembourg, Luxembourg

11 March 2013

What is complementation property

In DES, if you complement/flip all bits of plaintext and key, then all bits of ciphertext would flip

If $DES_K(P) = C$ then $DES_{\overline{K}}(\overline{P}) = \overline{C}$

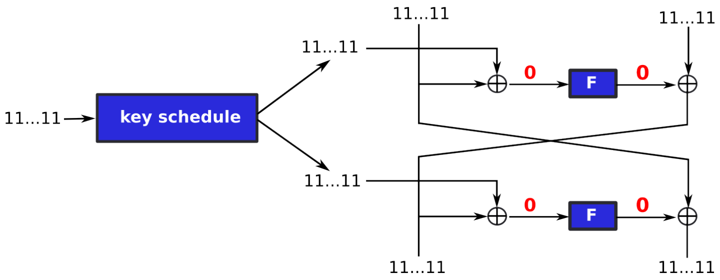
Results:

- Distinguisher with only two queries
- Reduction of exhaustive key search by factor 2

Why does it work

Complementation/ All bit flip = difference $11\ldots11$

- Diff. $11\ldots11$ in master key => diff. $11\ldots11$ in subkeys
- Difference $11\ldots11$ in the state and the subkey cancel



How to relax the requirements

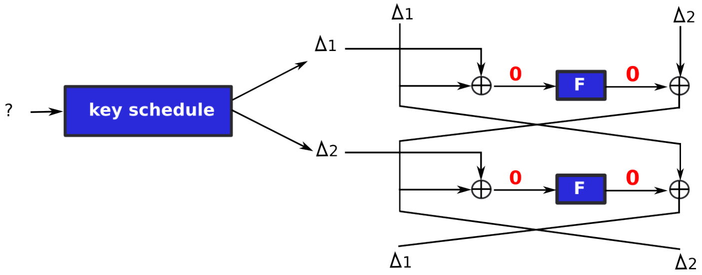
Original: If in Feistel cipher, for **any** key one flips **all** of the bits ...

Ideas for general:

- Not applicable to all keys, i.e. weak-key class
- Not necessarily flip all the bits

General complementation

- **Partial-alternating**: Start with (Δ_1, Δ_2) in the plaintext
- **Weak-key**: $KS(\Delta) \rightarrow (\Delta_1, \Delta_2, \ldots, \Delta_1, \Delta_2)$ for some K



Outcome

Lemma (Classical Feistel)

If for n-bit cipher with k-bit keys

$$\exists\Delta : KS(K \oplus \Delta) \oplus KS(K) \xrightarrow{p} (\Delta_1, \Delta_2, \Delta_1, \Delta_2, \ldots, \Delta_1, \Delta_2)$$

Then, if $p > 2^{-k}$, distinguisher for a weak-key class of size $p \cdot 2^k$ exists for the cipher.

- **Problem:** how to find the differential in the key schedule
- **Result:** RK differential where the state characteristic has probability 1

Outcome

Modular Feistel = subkeys are modularly added to the state

Lemma (Modular Feistel)

If for n-bit cipher with k-bit keys

$$\exists \Delta : KS(K \oplus \Delta) \oplus KS(K) \xrightarrow{p} (\Delta_1, \Delta_2, \Delta_1, \Delta_2, \ldots, \Delta_1, \Delta_2)$$

Then, if $p \cdot 2^{-\lceil \frac{r}{2} \rceil (|(\Delta_1)_{n-1}| + |(\Delta_2)_{n-1}|)} > 2^{-k}$ *and* $2^{-\lceil \frac{r}{2} \rceil (|(\Delta_1)_{n-1}| + |(\Delta_2)_{n-1}|)} > 2^{-n}$*, distinguisher for a weak-key class of size* $p \cdot 2^k$ *exists for the cipher.*

- **Problem:** how to find char. in the key schedule with low hamming weight output difference

Specification

Camellia-128 is Japanese CRYPTREC standard

- 128-bit state/key classical Feistel cipher with 2 additional non-linear layers
- 18 rounds
- Key schedule composed of 4 rounds of Feistels and rotations

We analyze the cipher without the non-linear layers !

Key schedule

- Intermediate key K_A is obtained from the master key K_L in four Feistel rounds
- All subkeys are particular 32-bit values of rotations of K_A, K_L on **various amounts**

The difference in the subkey has to be invariant of rotations => only choice is:

$$\Delta K_L \rightarrow \Delta K_A : 11\ldots11 \rightarrow 11\ldots11$$

Differential in the key schedule

- If we go with characteristic $11 \ldots 11 \rightarrow 11 \ldots 11$, the probability is too low as there are too many active S-boxes
- Switch to differentials:
  - compute the number of characteristics in the differential $11 \ldots 11 \rightarrow 11 \ldots 11$
  - compute the lower bound on probability of each characteristic
  - obtain the lower bound on probability of differential

Result: the differential has a probability of at least 2^{-128}, i.e. there is on good key

Applications

- Weak-key class is too small for attack on the cipher
- Switch to hash functions, e.g. Davies-Meyer mode based on Camellia-128
  - The right key/message can be found with 2^{112} encryptions
  - The right message produces collisions for any chaining value (key whitening introduces the right difference at the beginning and cancels the difference at the end)
  - *q*-differential multicollisions with 2^{112} calls for the *hash* function

Specification

GOST is Russian encryption standard

- 64-bit state, 256-bit key modular Feistel cipher
- 32 rounds
- No key schedule, only word permutations

NANYANG TECHNOLOGICAL UNIVERSITY

Key schedule and differentials

Master key words:

$$K_1, \ldots, K_8$$

Subkey words:

$$K_1, \ldots, K_8, K_1, \ldots, K_8, K_1, \ldots, K_8, K_8, \ldots, K_1$$

Probability 1 differential for any difference in the master key words

Complementing GOST

Complementation property of GOST has been known and used in previous analysis !

- RK distinguisher with difference 2^{31} in all master key words
- Key-recovery with difference 2^t in all master key words

Attacks that recover the full key have impractical complexity

Complementing GOST

We use:

- Simple key schedule
- Probability of key schedule differential is 1
- Prob. of one round Feistel with one same active bit in state and subkey is 2^{-1}
- If bits cancelled and input is known then subkey bit can be determined

Key recovery on GOST

- **Data generation:** For each 31 related pair $(K, K \oplus 2^i)$ encrypt 2^{32} plaintext pairs $(P, P \oplus 2^i)$
- **Data collection:** For each i find the pair of ciphertexts $(C, C \oplus 2^i)$ – 31 pairs in total
- **Domino effect:**
  - Recover 31-bits of the current round (one bit from each of the 31 pairs)
  - Guess the MSB, compute the new state, repeat the process

Key recovery on GOST

- Framework: related-key attack with 31 related key pairs
- Data complexity: $31 \times 2 \times 2^{32} \approx 2^{38}$
- Time complexity: 2^{38} (data generation) $+ 2^{8}$ (domino) $\approx 2^{38}$
- Result: **full 256-bit key recovery**

Both complexities are practicals – our implementation on a PC with a single core and non-optimized code recovered the full key in one day

Conclusion

- General complementation can help finding (easier) RK differential attacks – focus only on key schedule
- #rounds does not matter for classical Feistel
- Applicable to Generalized Feistels as well
- Should not be used to “prove” resistance against differential attacks !

Conclusion

- General complementation can help finding (easier) RK differential attacks – focus only on key schedule
- #rounds does not matter for classical Feistel
- Applicable to Generalized Feistels as well
- Should not be used to "prove" resistance against differential attacks !

Stay tuned for our Rump Session talk on complementing full-round CLEFIA