Cryptanalysis of GOST2

Tomer Ashur, Achiya Bar-On, Orr Dunkelman

February 22, 2017

Outline

- A brief description of GOST and GOST2

Outline

- A brief description of GOST and GOST2
- A weak-key reflection attack on GOST2

Outline

- A brief description of GOST and GOST2
- A weak-key reflection attack on GOST2
- An impossible reflection attack on GOST2

Outline

- A brief description of GOST and GOST2
- A weak-key reflection attack on GOST2
- An impossible reflection attack on GOST2
- A fixed point attack on GOST2

Description of GOST

- Designed by the Soviet Union

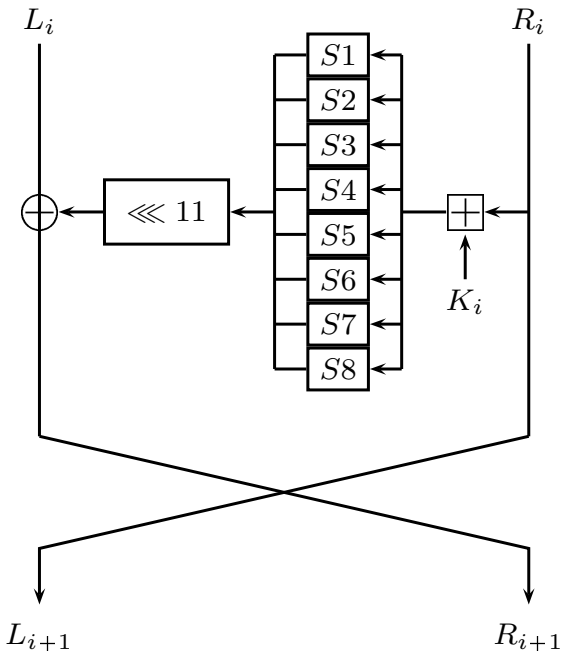
Description of GOST

- Designed by the Soviet Union
- Balanced Feistel structure; 64-bit block; 256-bit key; 8 S-boxes

Description of GOST

- Designed by the Soviet Union
- Balanced Feistel structure; 64-bit block; 256-bit key; 8 S-boxes
- Keys are injected in ascending cyclic order in rounds 0-23, and in a descending order in rounds 24-32.

GOST's Round Function



GOST's Key Order

Round	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Subkey (GOST)	K^0	K^1	K^2	K^3	K^4	K^5	K^6	K^7	K^0	K^1	K^2	K^3	K^4	K^5	K^6	K^7
Round	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Subkey (GOST)	K^0	K^1	K^2	K^3	K^4	K^5	K^6	K^7	K^7	K^6	K^5	K^4	K^3	K^2	K^1	K^0

Related Work

- Weak-key reflection attack [Kar08]

Related Work

- Weak-key reflection attack [Kar08]
- Reflection attack [Iso11]

Related Work

- Weak-key reflection attack [Kar08]
- Reflection attack [Iso11]
- Fixed point [DDS12]

GOST2's Key Order

Round	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Subkey (GOST2)	K^0	K^1	K^2	K^3	K^4	K^5	K^6	K^7	K^3	K^4	K^5	K^6	K^7	K^0	K^1	K^2
Round	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Subkey (GOST2)	K^5	K^6	K^7	K^0	K^1	K^2	K^3	K^4	K^6	K^5	K^4	K^3	K^2	K^1	K^0	K^7

A Weak-key Reflection Attack - Preliminaries

- In a Feistel structure, decryption is the same procedure as encryption with the left and right sides exchanged and a different key order

A Weak-key Reflection Attack - Preliminaries

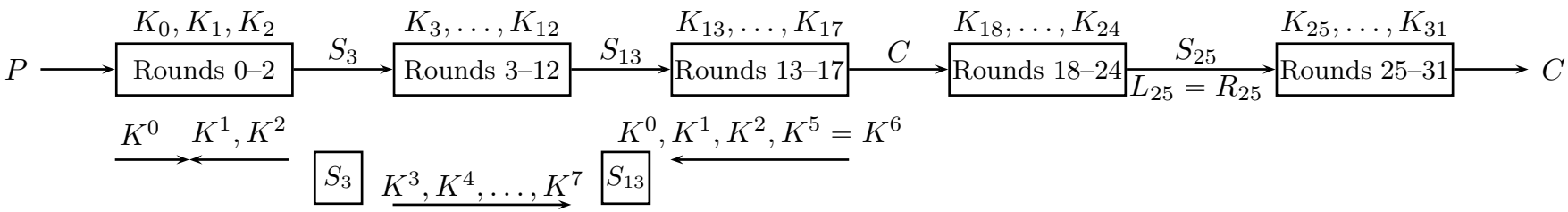
- In a Feistel structure, decryption is the same procedure as encryption with the left and right sides exchanged and a different key order
- When the left and the right sides are the same, only the keys matter

- In a Feistel structure, decryption is the same procedure as encryption with the left and right sides exchanged and a different key order
- When the left and the right sides are the same, only the keys matter
- If S is a reflection point, then for any key $R_k(S) = R_k^{-1}(S)$

A Weak-key Reflection Attack - Key Order

Round	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Subkey (GOST2)	K^0	K^1	K^2	K^3	K^4	K^5	K^6	K^7	K^3	K^4	K^5	K^6	K^7	K^0	K^1	K^2
Round	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Subkey (GOST2)	K^5	K^6	K^7	K^0	K^1	K^2	K^3	K^4	$\mathbf{K^6} =$	$\mathbf{K^5}$	K^4	K^3	K^2	K^1	K^0	K^7

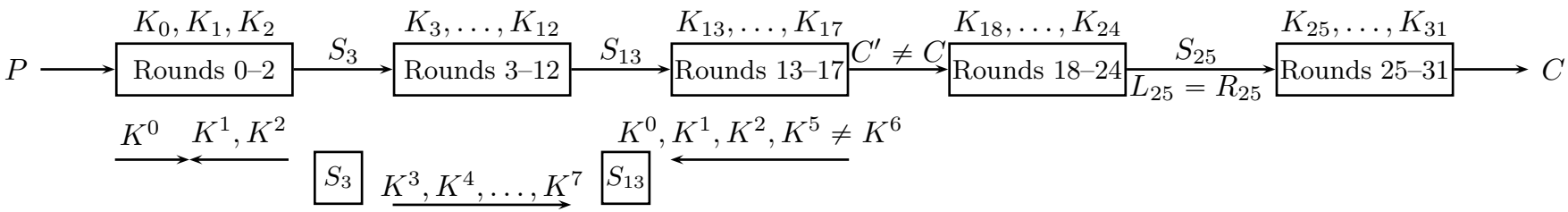
A Weak-key Reflection Attack - Description



A Weak-key Reflection Attack - Complexity

- Size of weak-key class: 2^{224}
- Time complexity: 2^{192}
- Data complexity: 2^{32} known plaintexts
- Memory complexity: $2^{68.58}$ bytes

An Impossible Reflection Attack



An Impossible Reflection Attack - Complexity

- Number of impossible keys: $(2e)^{-1}$
- Time complexity: $2^{254.34}$
- Data complexity: 2^{63} chosen plaintexts
- Memory complexity: $2^{166.58}$ bytes

A Fixed-point Attack - Preliminaries

- A fixed point is a state S such that $S = F(S)$.

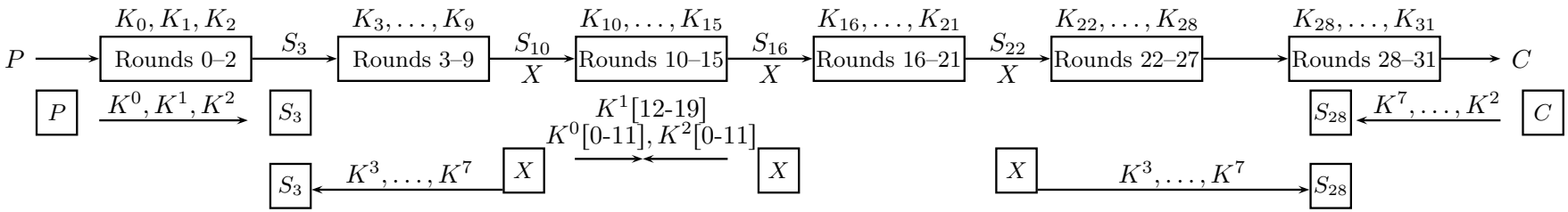
A Fixed-point Attack - Preliminaries

- A fixed point is a state S such that $S = F(S)$.
- The probability to observe a fixed point is 2^{-64}

A Fixed-point Attack - Key Ordering

Round	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Subkey (GOST2)	K^0	K^1	K^2	K^3	K^4	K^5	K^6	K^7	K^3	K^4	K^5	K^6	K^7	K^0	K^1	K^2
Round	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Subkey (GOST2)	K^5	K^6	K^7	K^0	K^1	K^2	K^3	K^4	K^6	K^5	K^4	K^3	K^2	K^1	K^0	K^7

A Fixed Point Attack



A Fixed Point Attack - Complexity

- Time complexity: 2^{237}
- Data complexity: 2^{64} known plaintexts
- Memory complexity: $2^{138.15}$ bytes

Summary

- Weak-key reflection attack

Summary

- Weak-key reflection attack
- Impossible reflection attack

Summary

- Weak-key reflection attack
- Impossible reflection attack
- Fixed point attack

Summary

- Weak-key reflection attack
- Impossible reflection attack
- Fixed point attack
- Related-key differential characteristics

Thank you