Cryptanalysis of C2

Julia Borghoff, Lars R. Knudsen, Gregor Leander, Krystian Matusiewicz

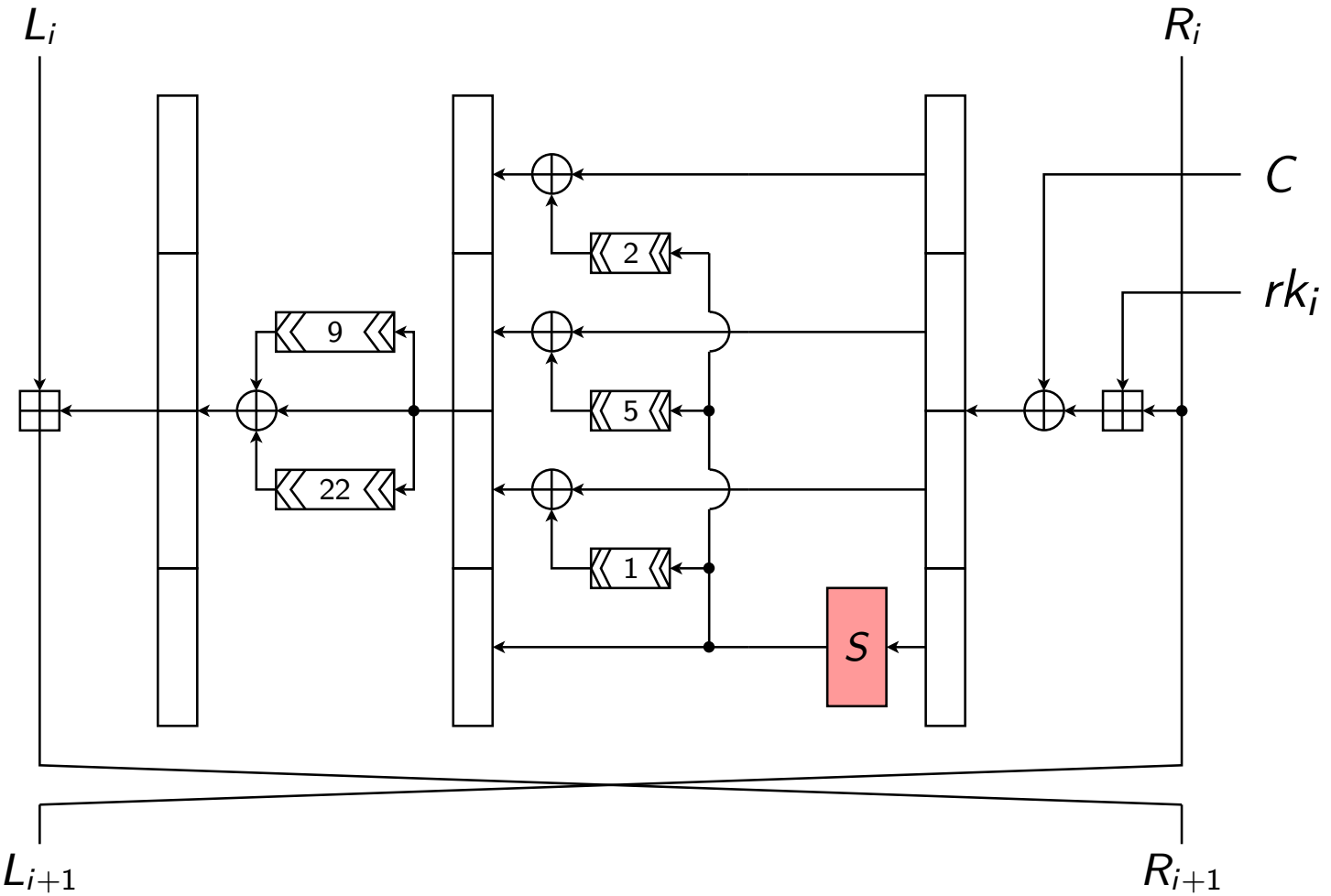
CRYPTO 2009

The block cipher C2

- 64-bit block cipher with 56-bit key
- **8-to-8 S-box is kept secret $\Rightarrow$ 2048 additional secret bits**
- 10-round Feistel cipher
- Designed by 4C Entity (IBM, Intel, Matsushita and Toshiba)
- Used in CPRM/CPPM Digital Rights Management scheme
- DVD-Audio, SD-cards

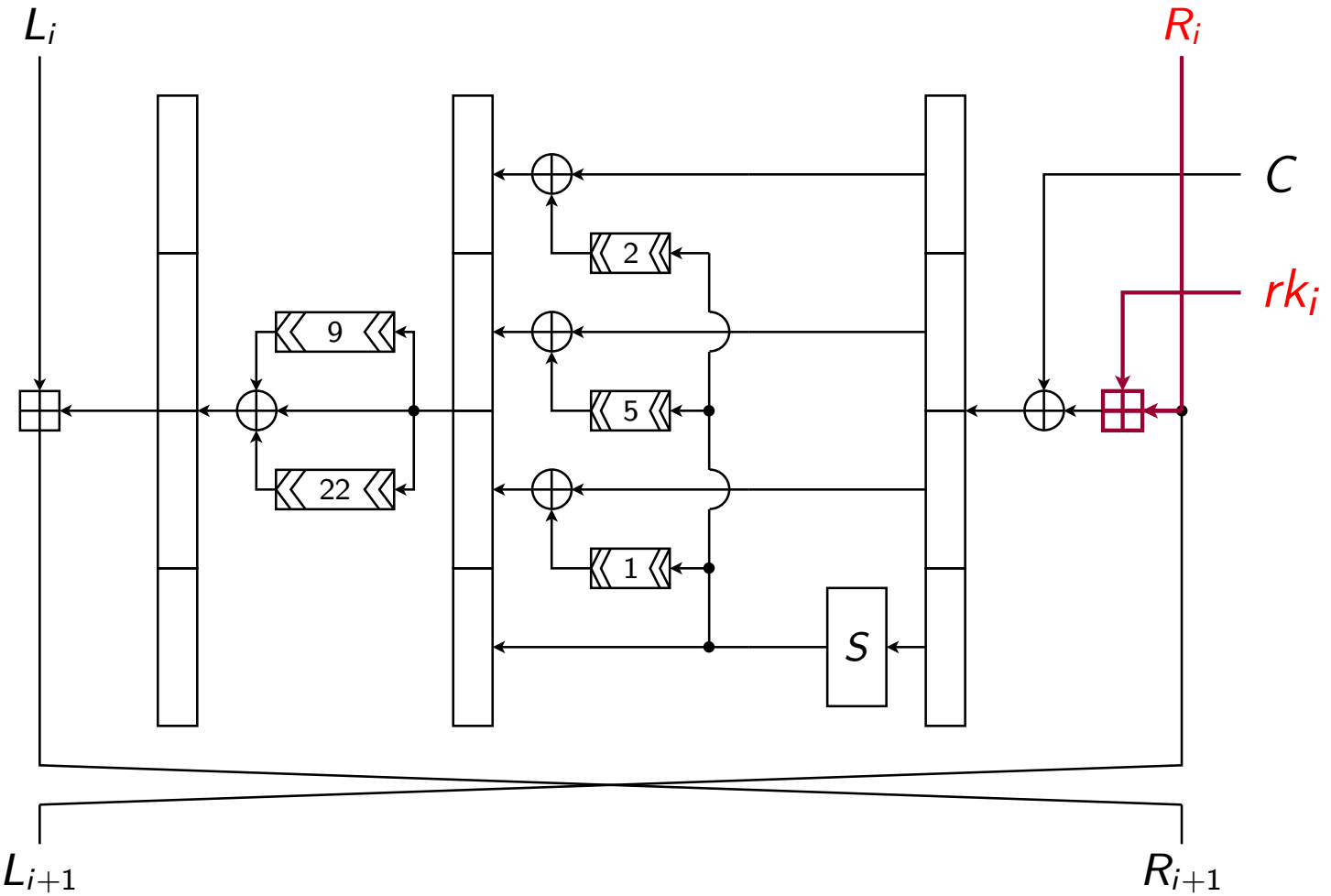
C2: round function

- 10 Feistel rounds



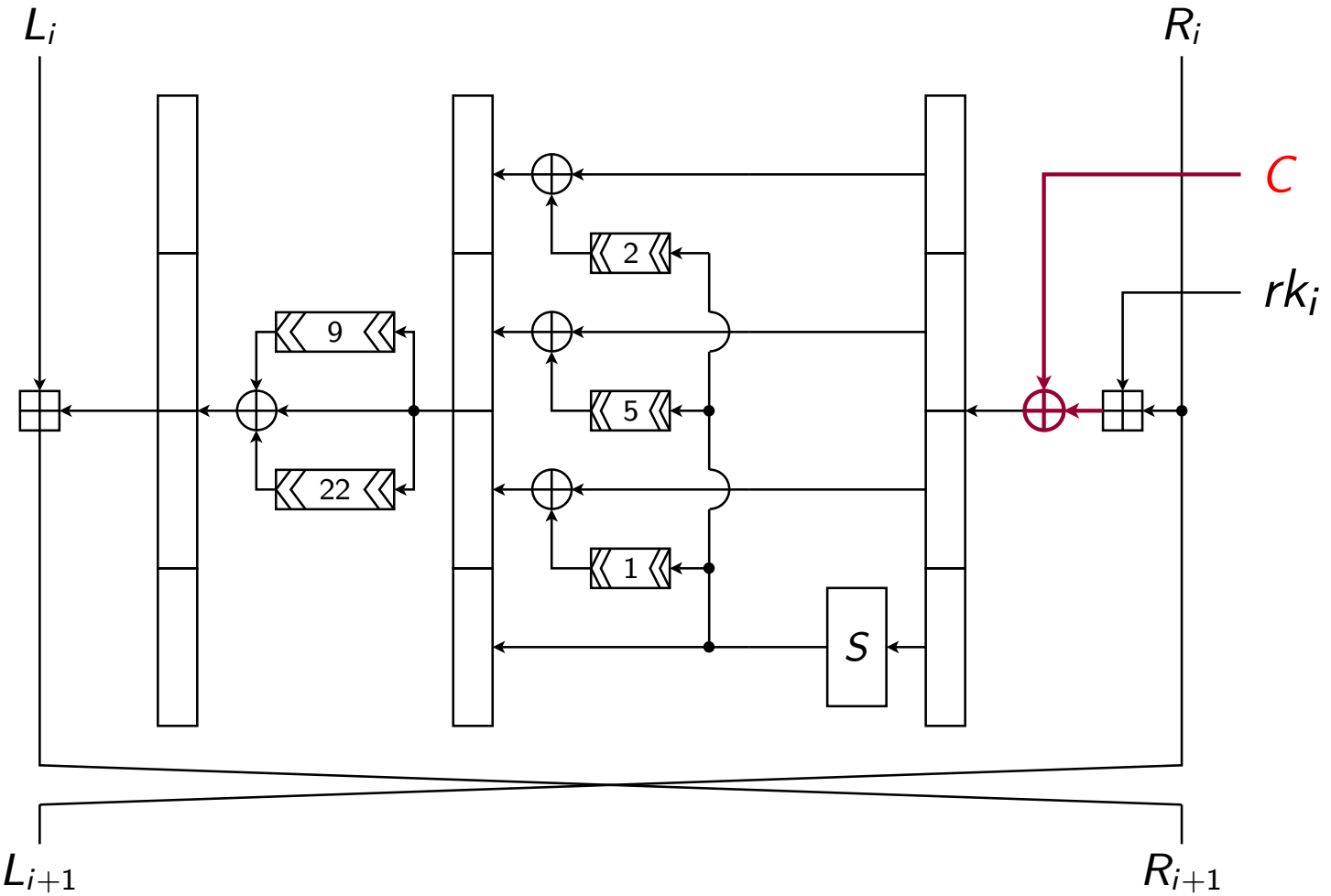
C2: round function

- 10 Feistel rounds



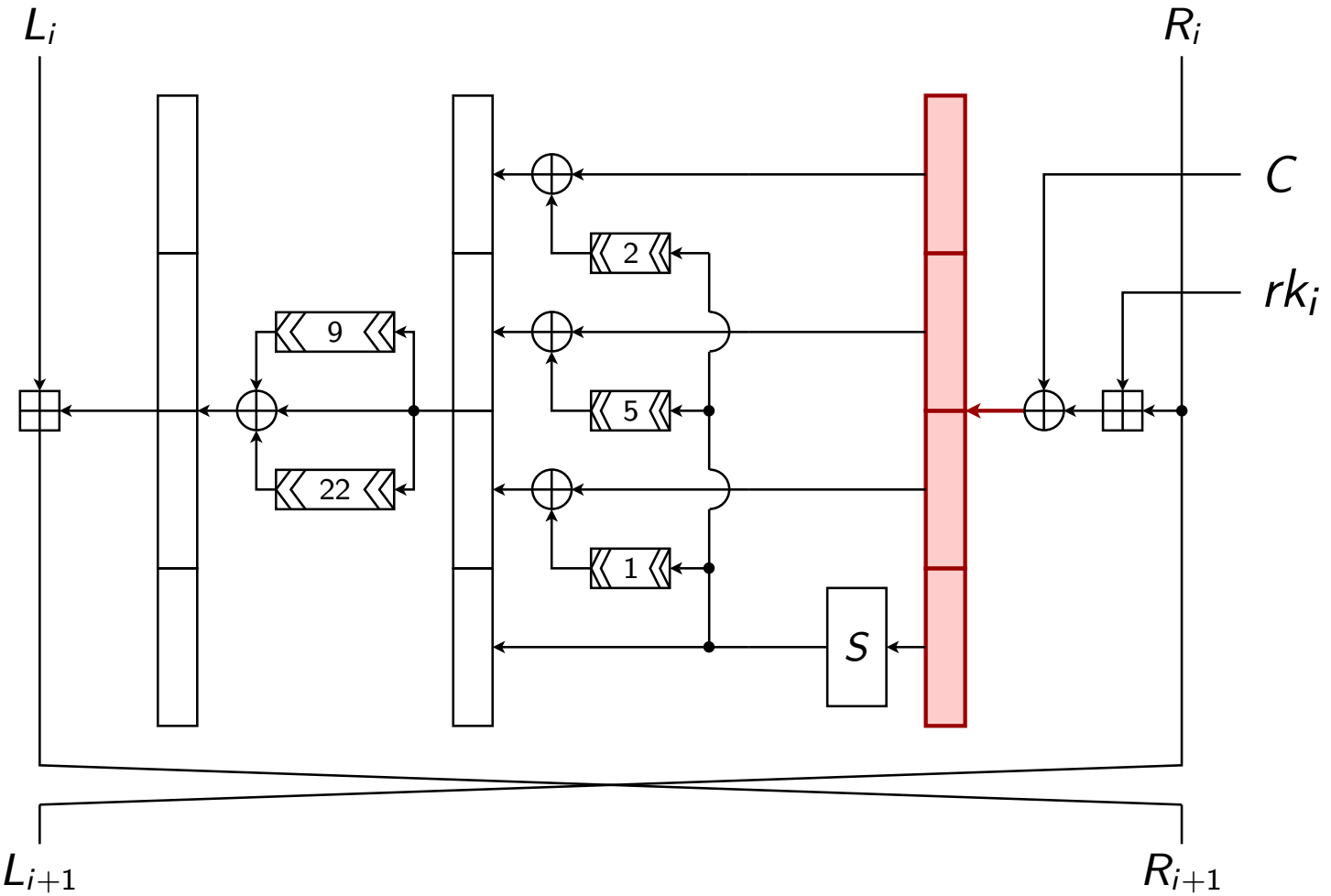
C2: round function

- 10 Feistel rounds



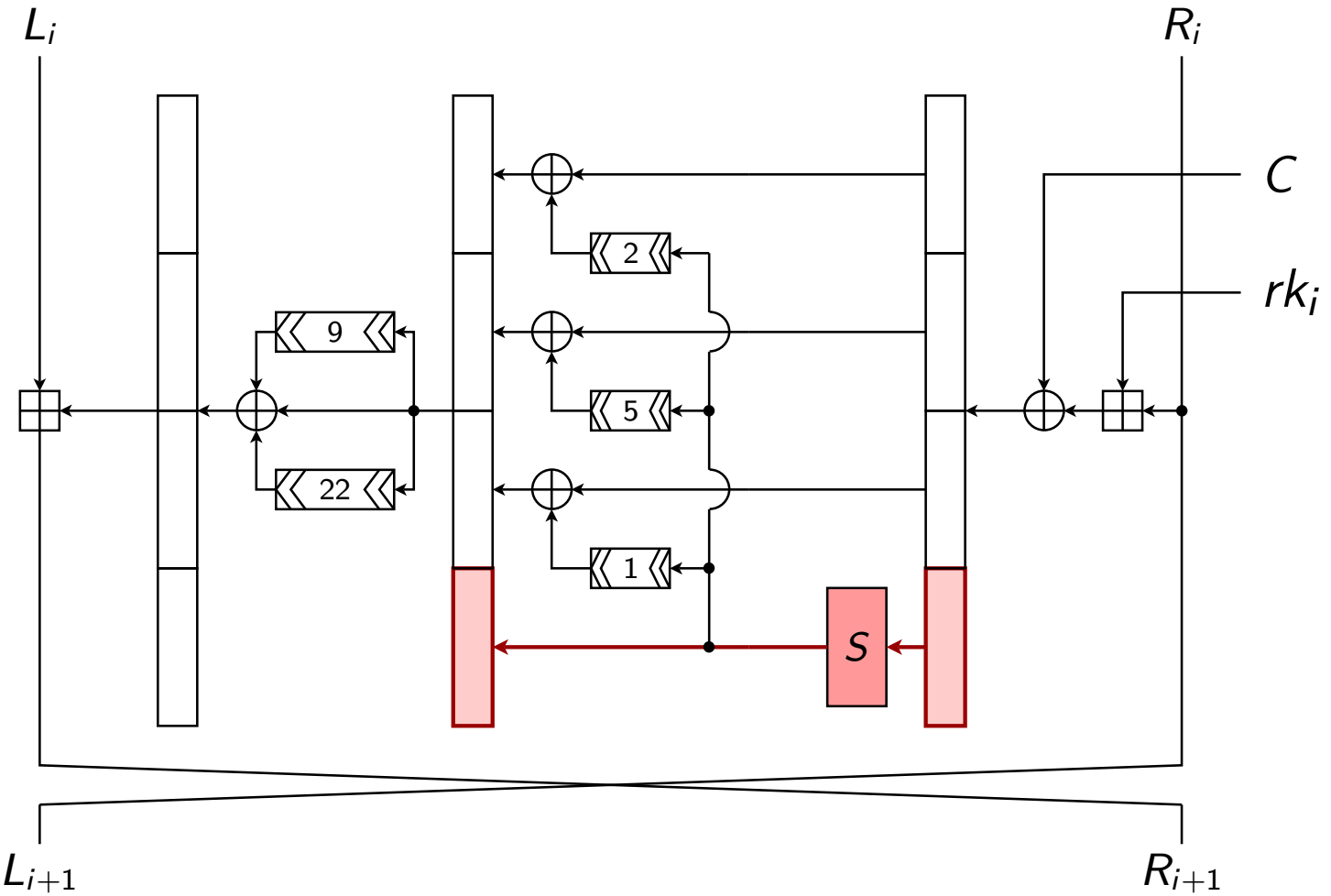
C2: round function

- 10 Feistel rounds



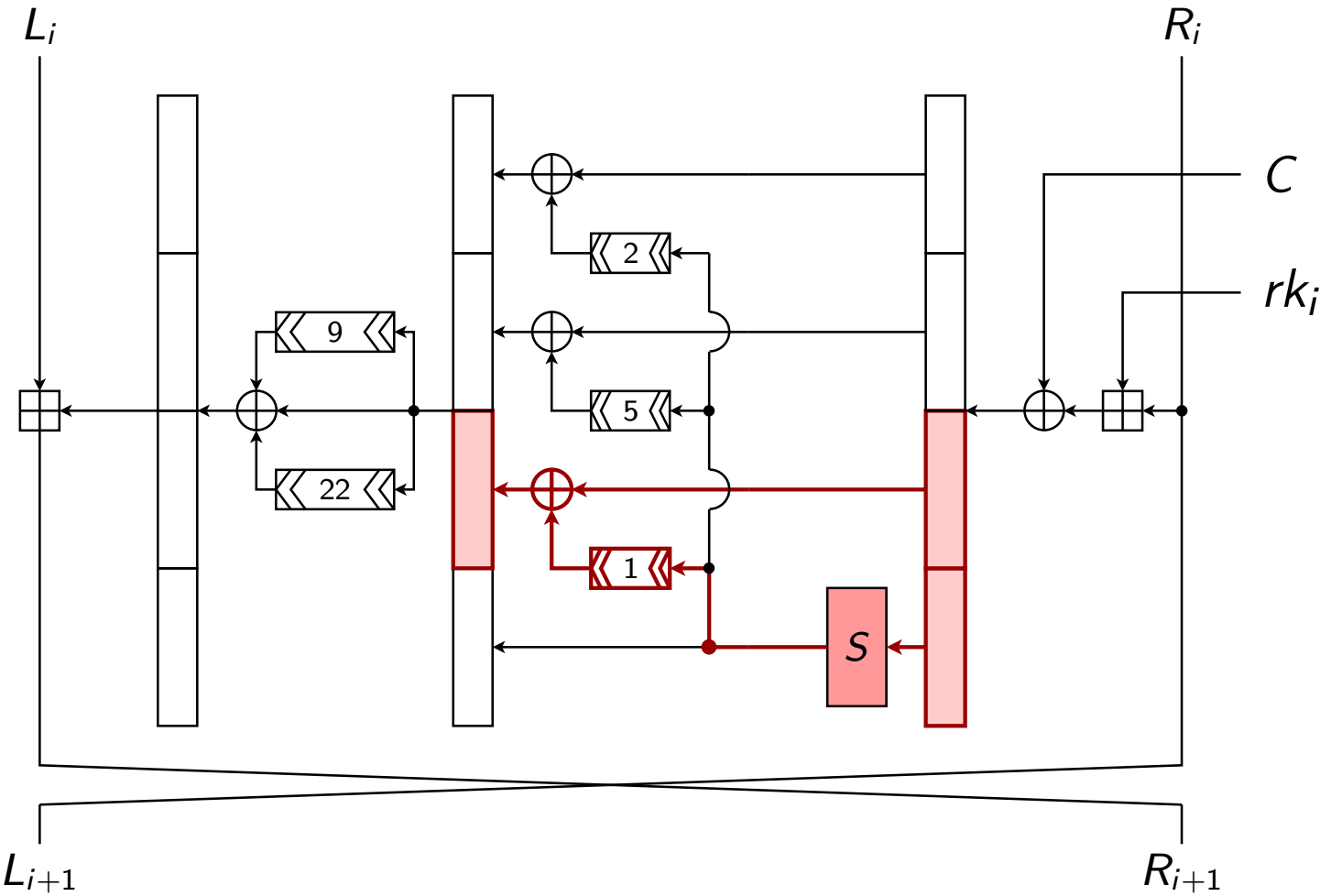
C2: round function

- 10 Feistel rounds



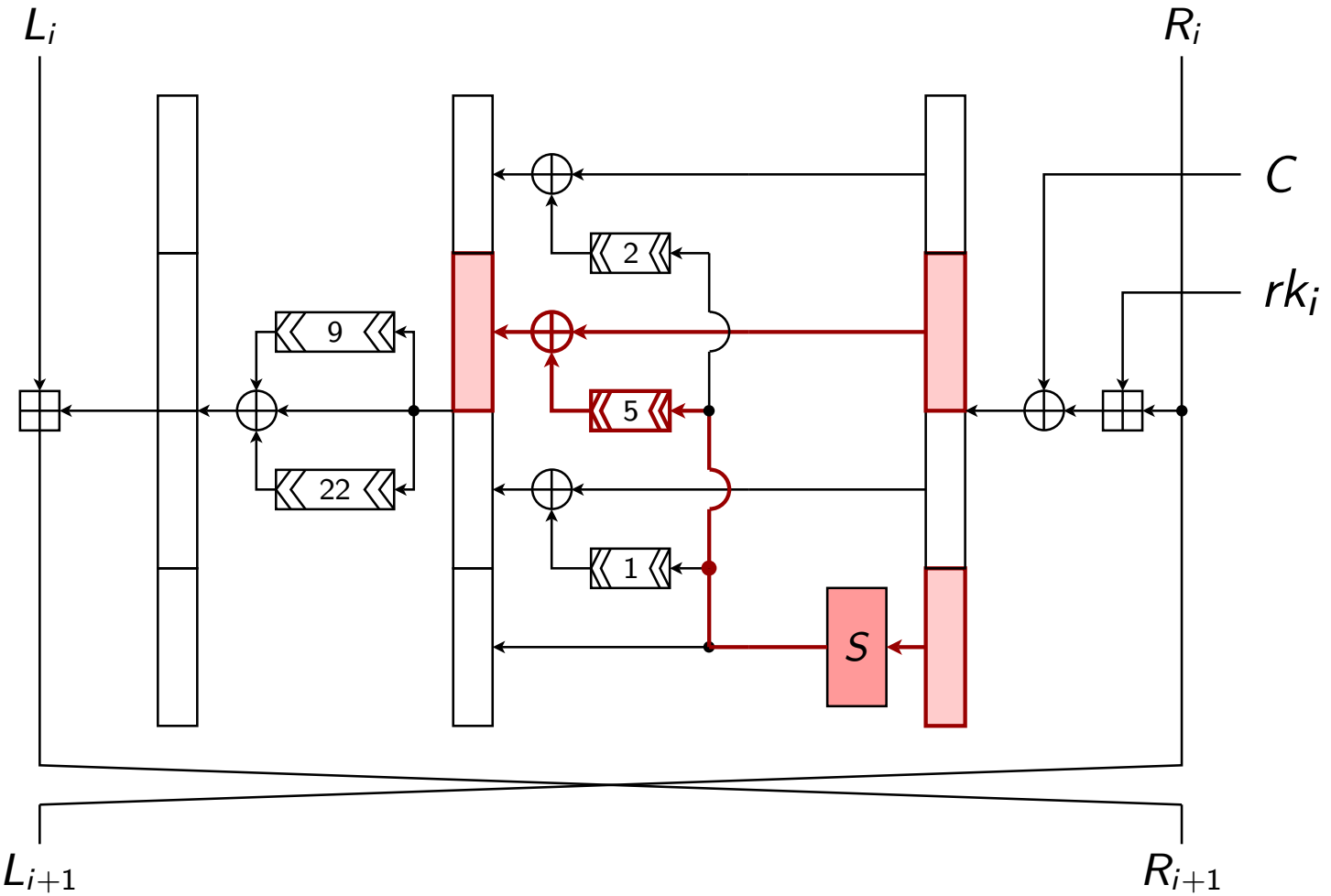
C2: round function

- 10 Feistel rounds



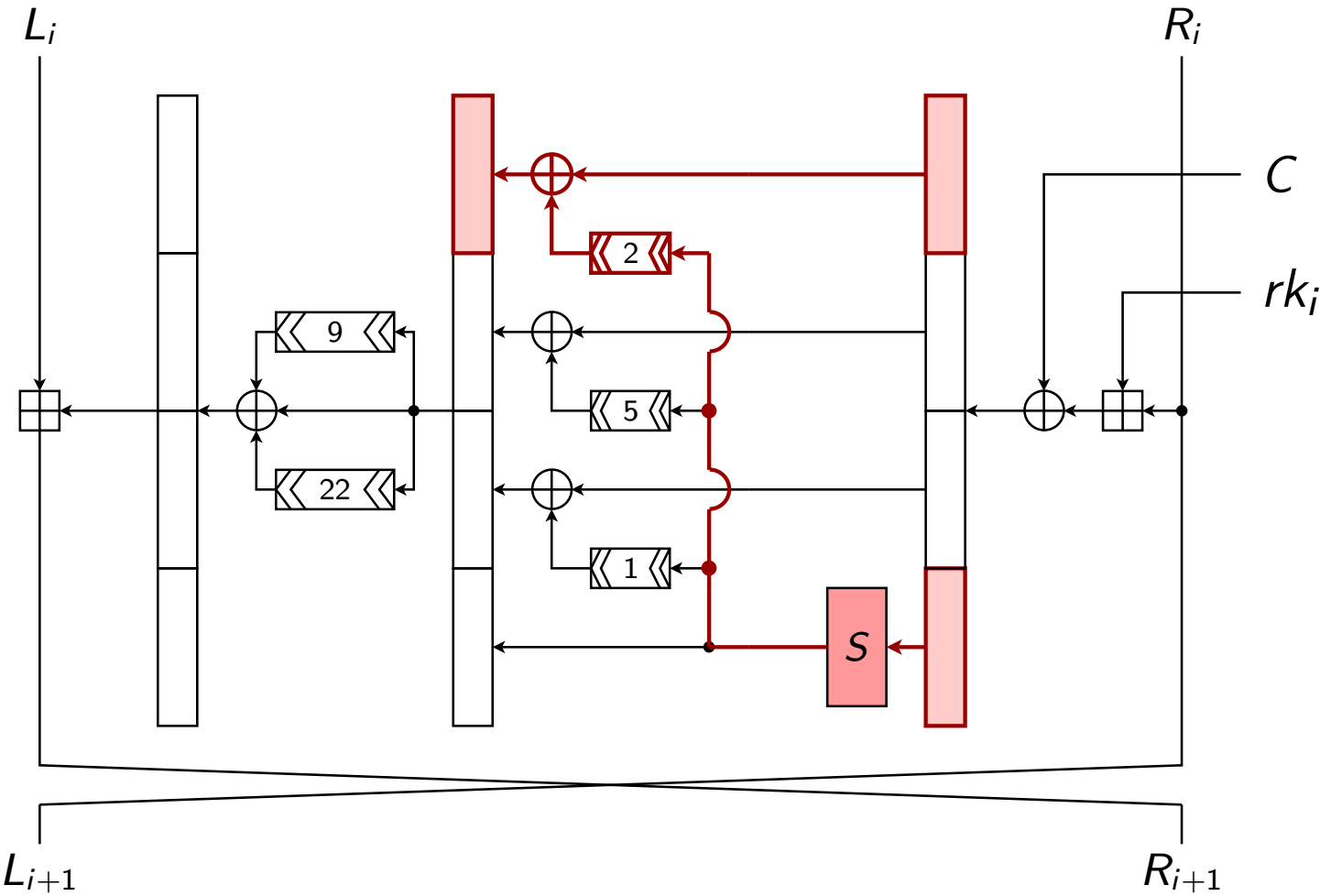
C2: round function

- 10 Feistel rounds



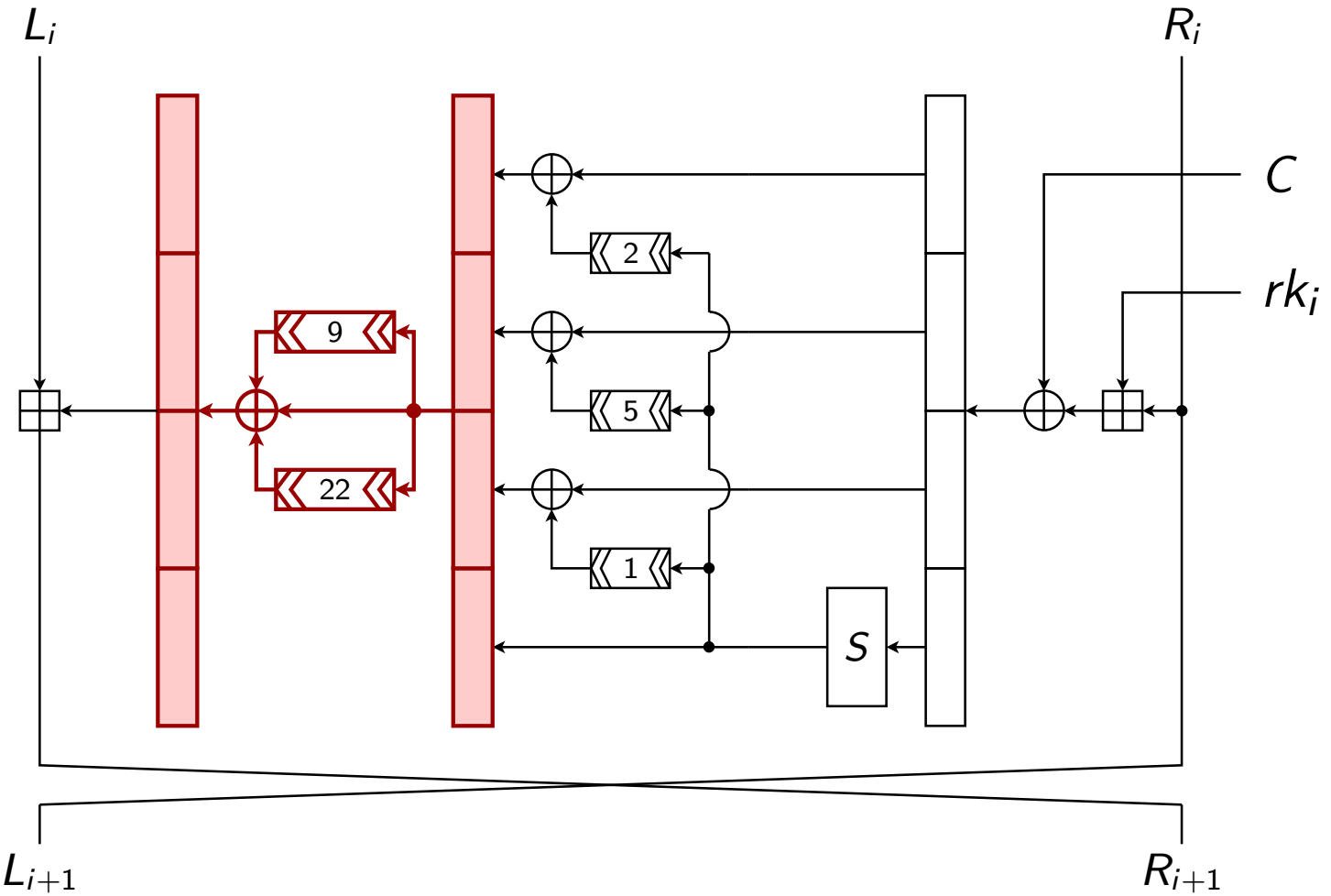
C2: round function

- 10 Feistel rounds



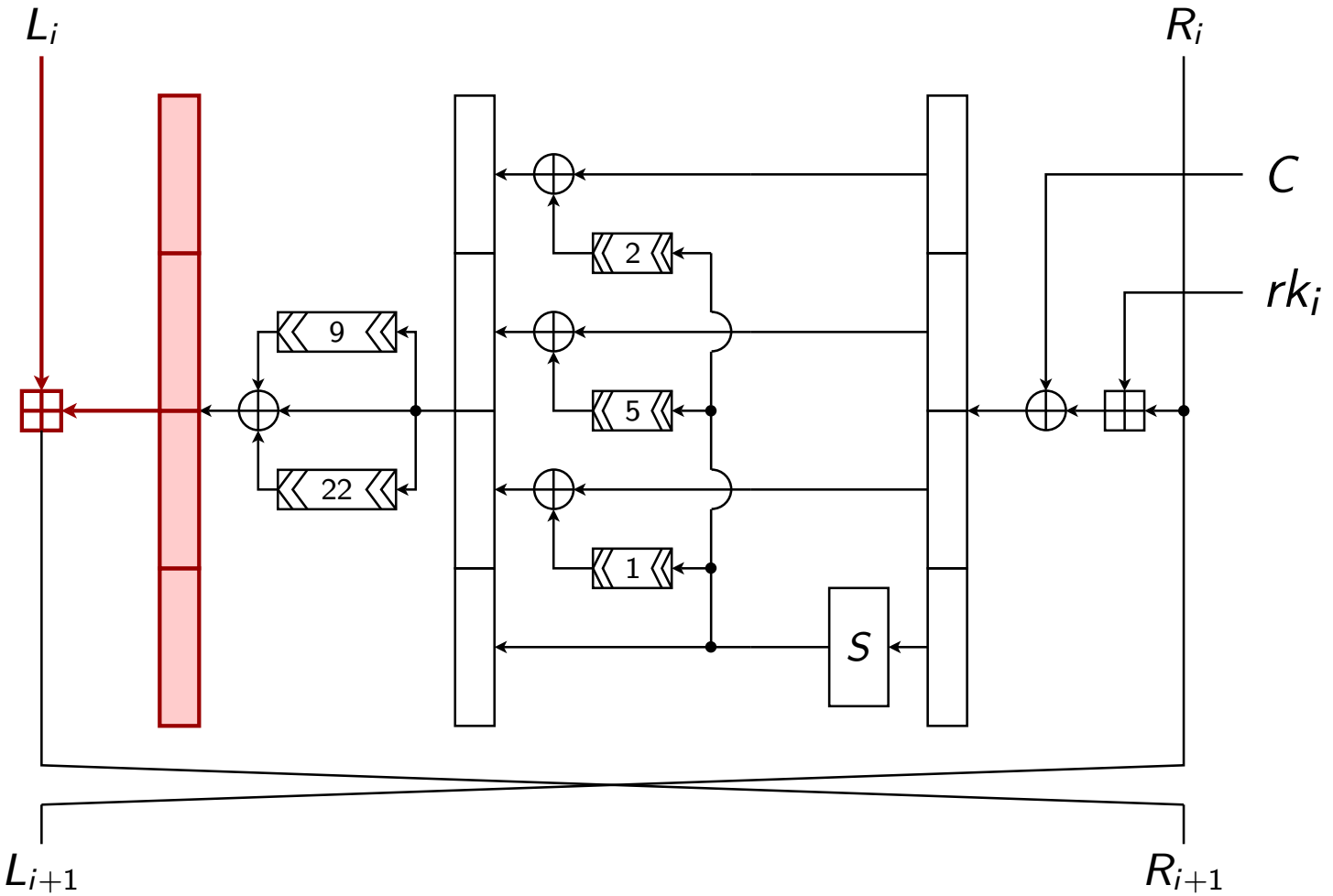
C2: round function

- 10 Feistel rounds



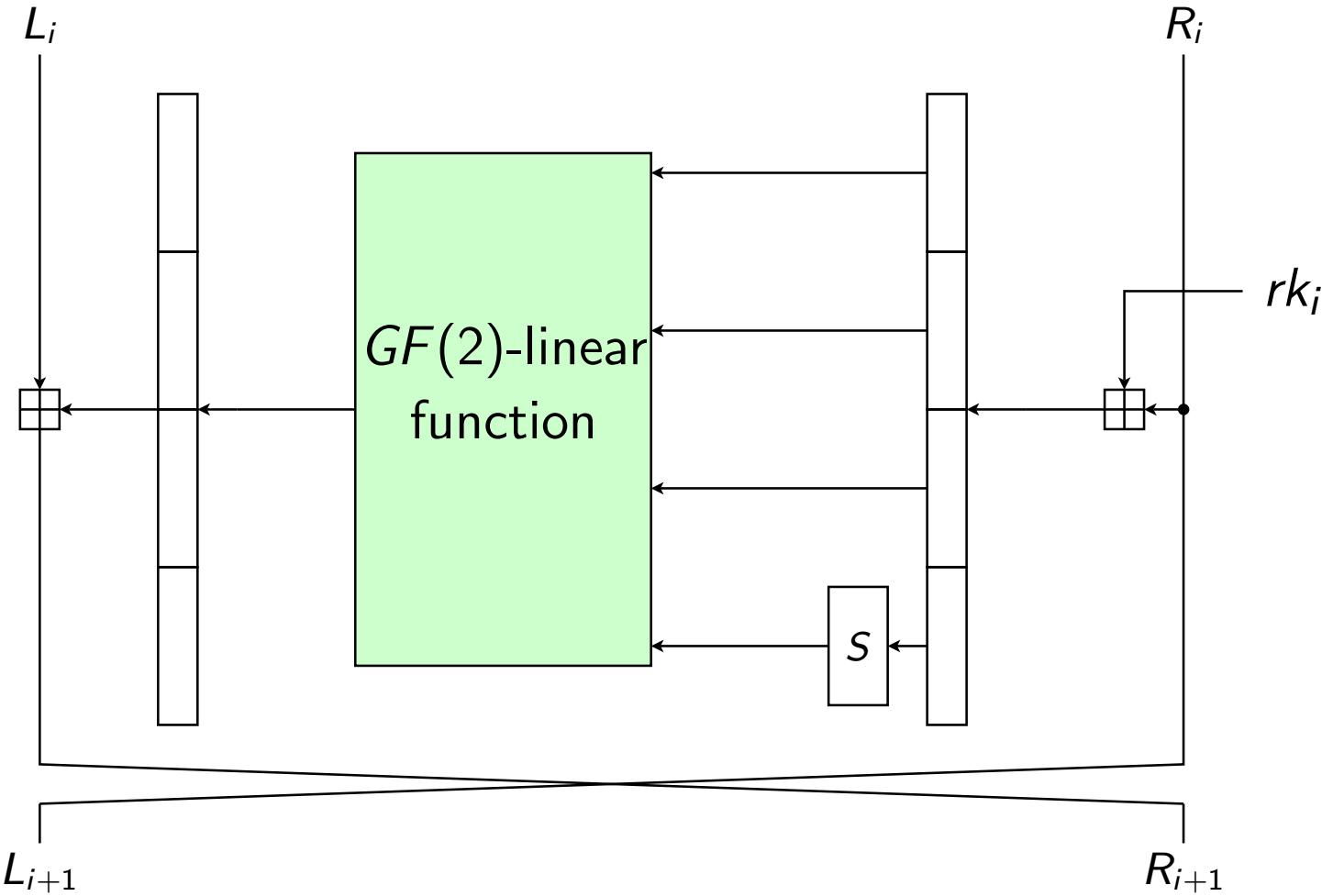
C2: round function

- 10 Feistel rounds



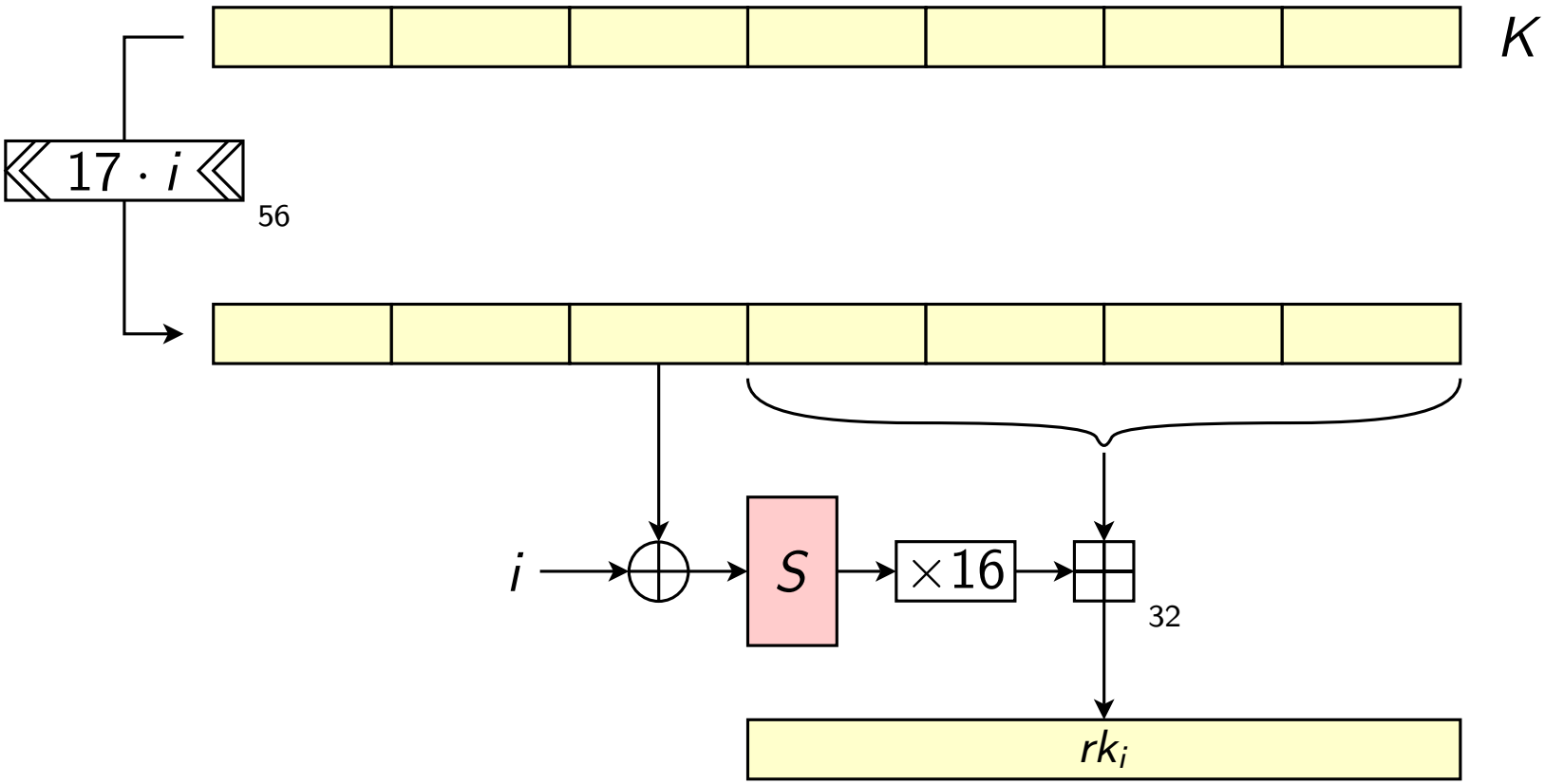
C2: round function

- The $GF(2)$-linear part is not relevant for the attack



C2: key scheduling

Produces 10 round keys rk_i out of 56-bit master key K



Possible attacks

There are three possible attack scenarios

	provided we can ...	recover
1.	set the key and query the device	S-box
2.	query the device and know the S-box	the secret key
3.	query the device	S-box and secret key

Previous work

- Japanese distributed cracking effort in 2004. Brute force over key space for a guessed S-box.
  Guess was wrong and the project failed.
- Algebraic S-box recovery attack for 8 out of 10 rounds (R.-P. Weinmann).

Complexity

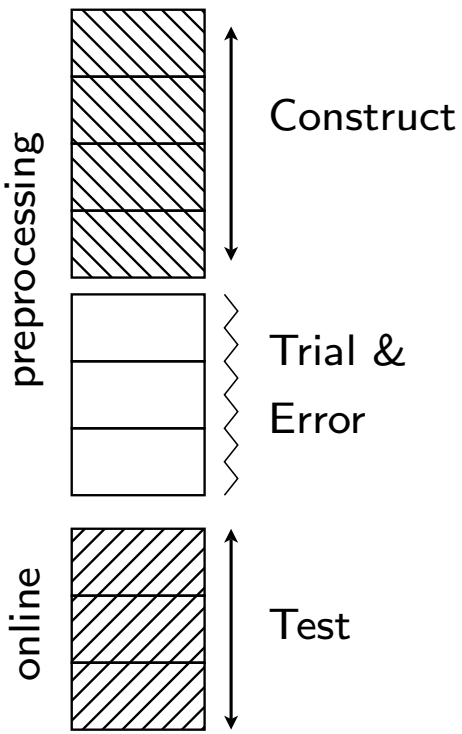
The three attacks and their complexities

	provided we can ...	recover	complexity
1.	set key + query device	S-box	2^{24}
2.	query device + know S-box	key	2^{48}
3.	query the device	S-box +key	$2^{53.5}$

Idea of attack 1

- One encryption generates 20 inputs to the S-box
  10 in the key schedule
  10 in the encryption algorithm
- There are $2^{20\times 8} = 2^{160}$ possibilities if we guess the S-box entries.
- Try to minimize the S-box entries we have to guess

Outline of the attack 1



- Preprocessing-phase
  - masterkeys which generate only 3 distinct S-box inputs in key schedule
  - Find plaintexts which generate only the same 3 S-box inputs in first 7 rounds
- Online-phase
  - Encrypt each plaintext (one plaintext for each guess of the S-box outputs)
  - Check if the ciphertext after 7 rounds is the expected.
  - If yes, determine 3 S-box entries.

Master key

Fix the master key to

`0x40, 0x84, 0x88, 0x40, 0x02, 0x80,0x09.`

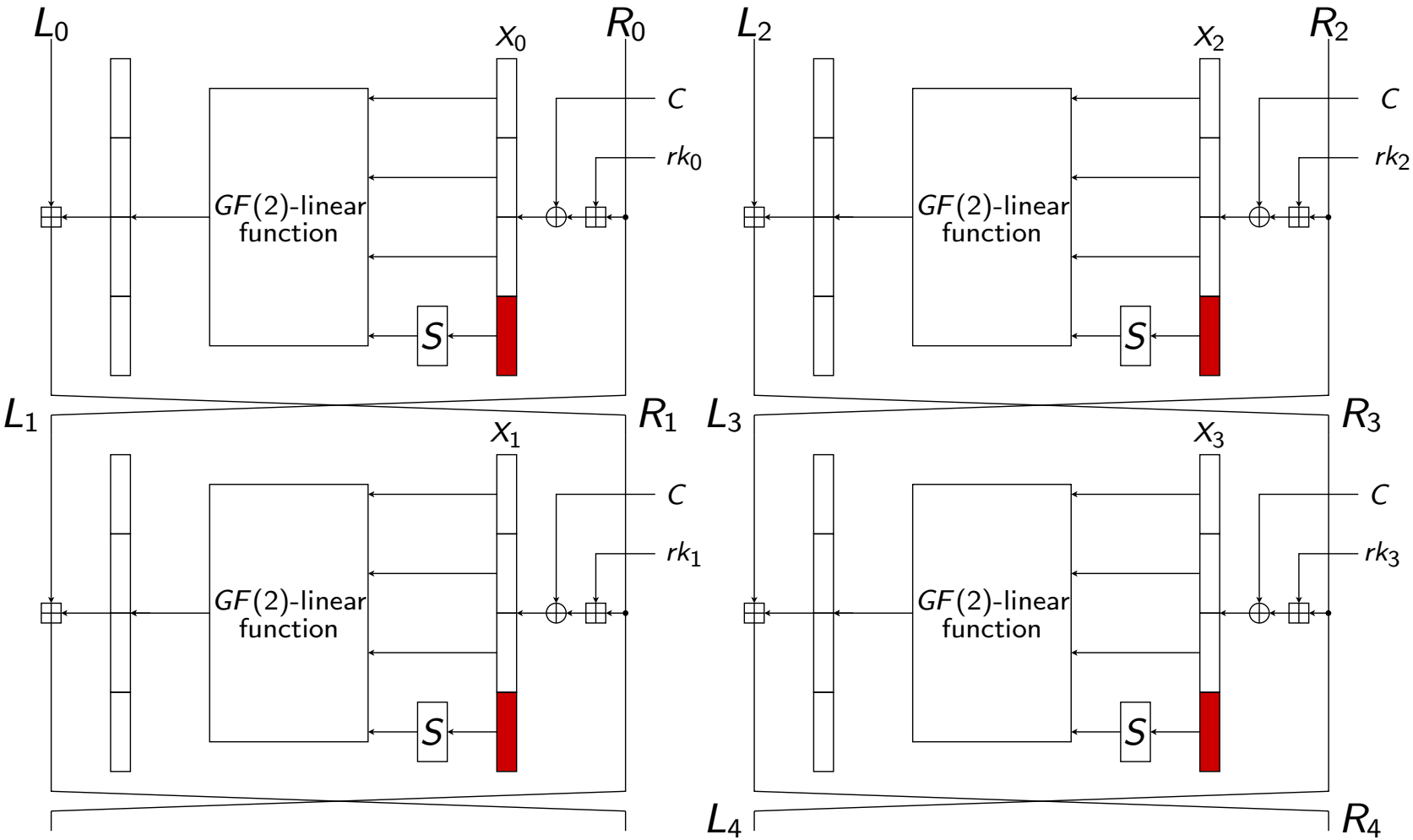
This key generates only the inputs

`0x88, 0x04, 0x27, 0x27, 0x04, 0x04, 0x27, 0x27, 0x88, 0x88`

to the S-box in the key schedule.

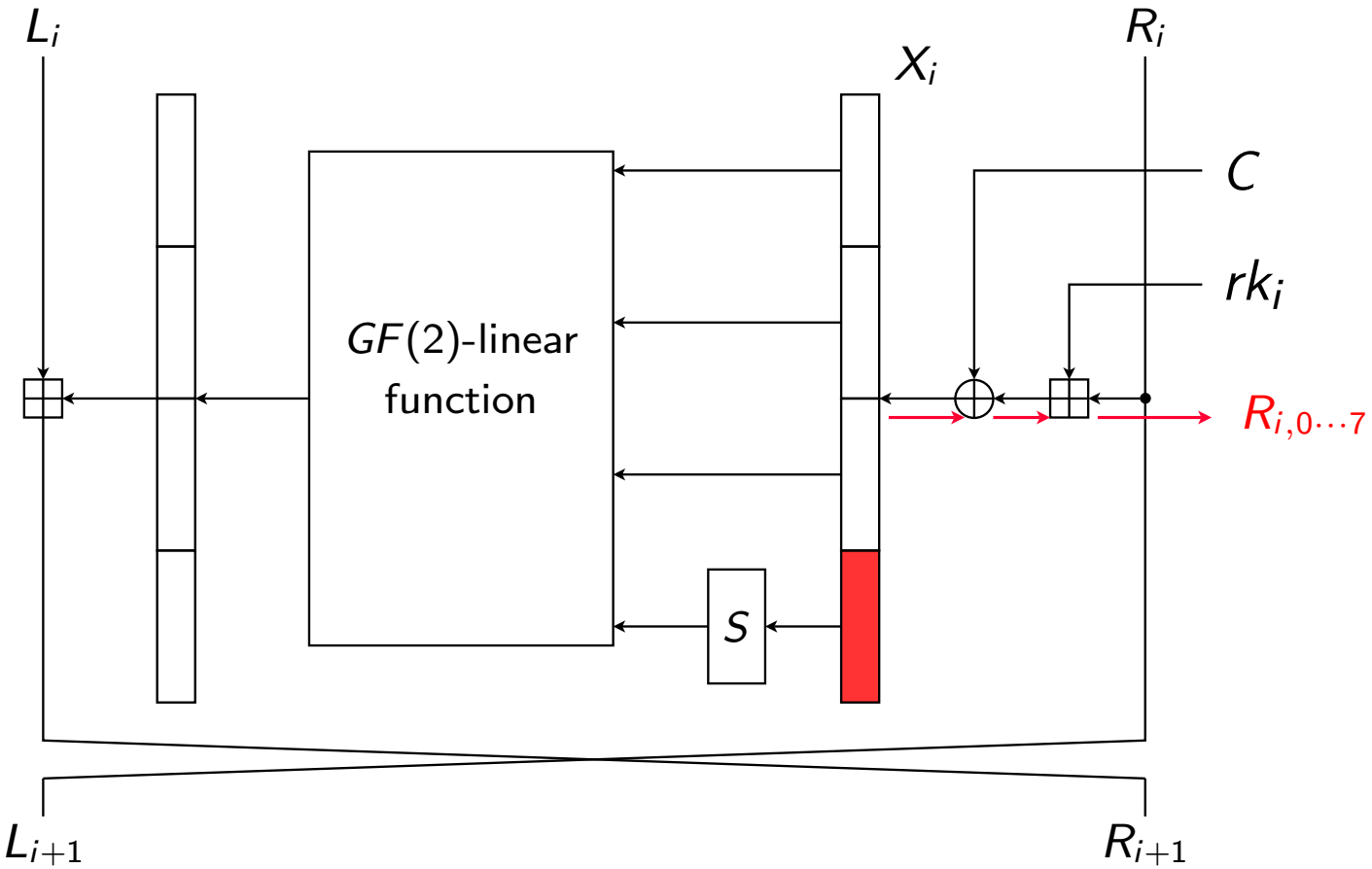
Generating plaintexts

- Fix the input to the S-boxes of 4 rounds



Generating plaintexts

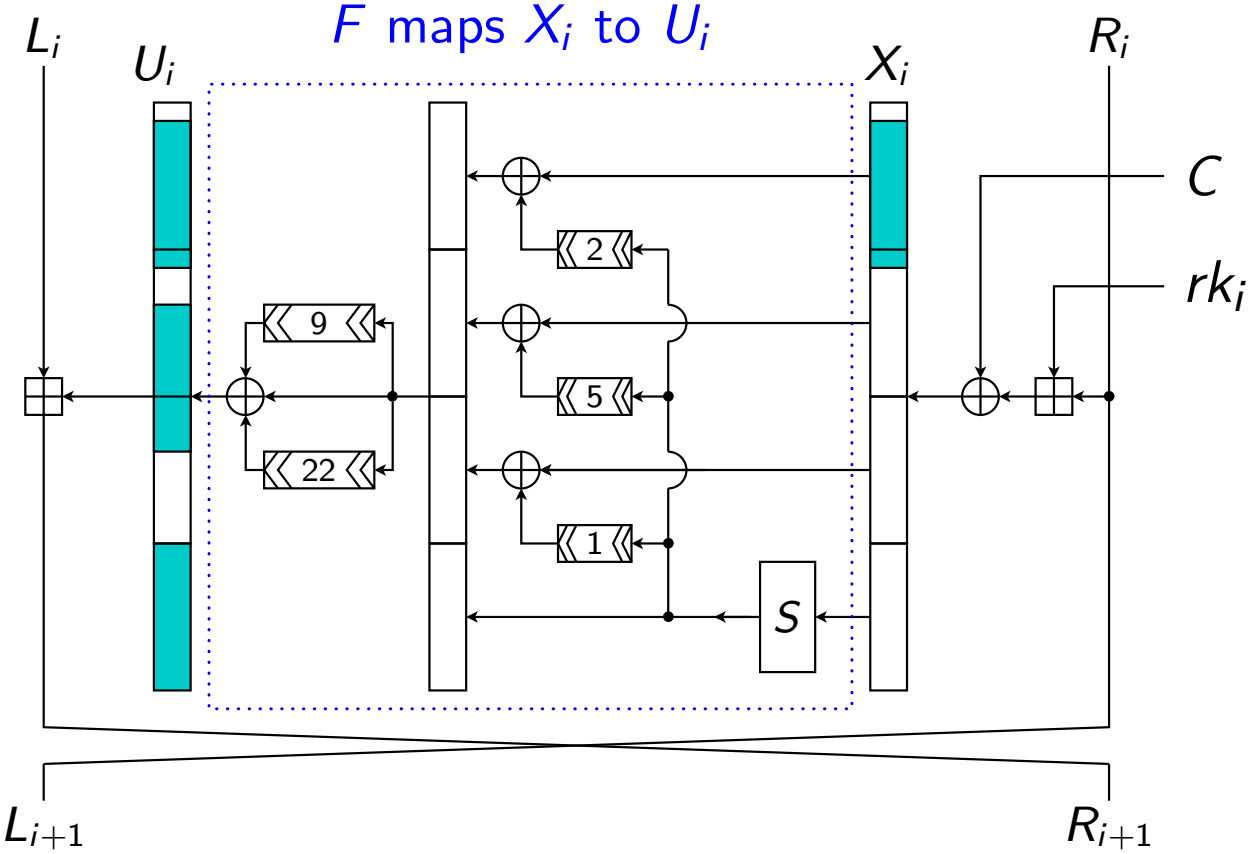
- Calculate backwards



Generating plaintexts

- For every 8-bit vector z holds

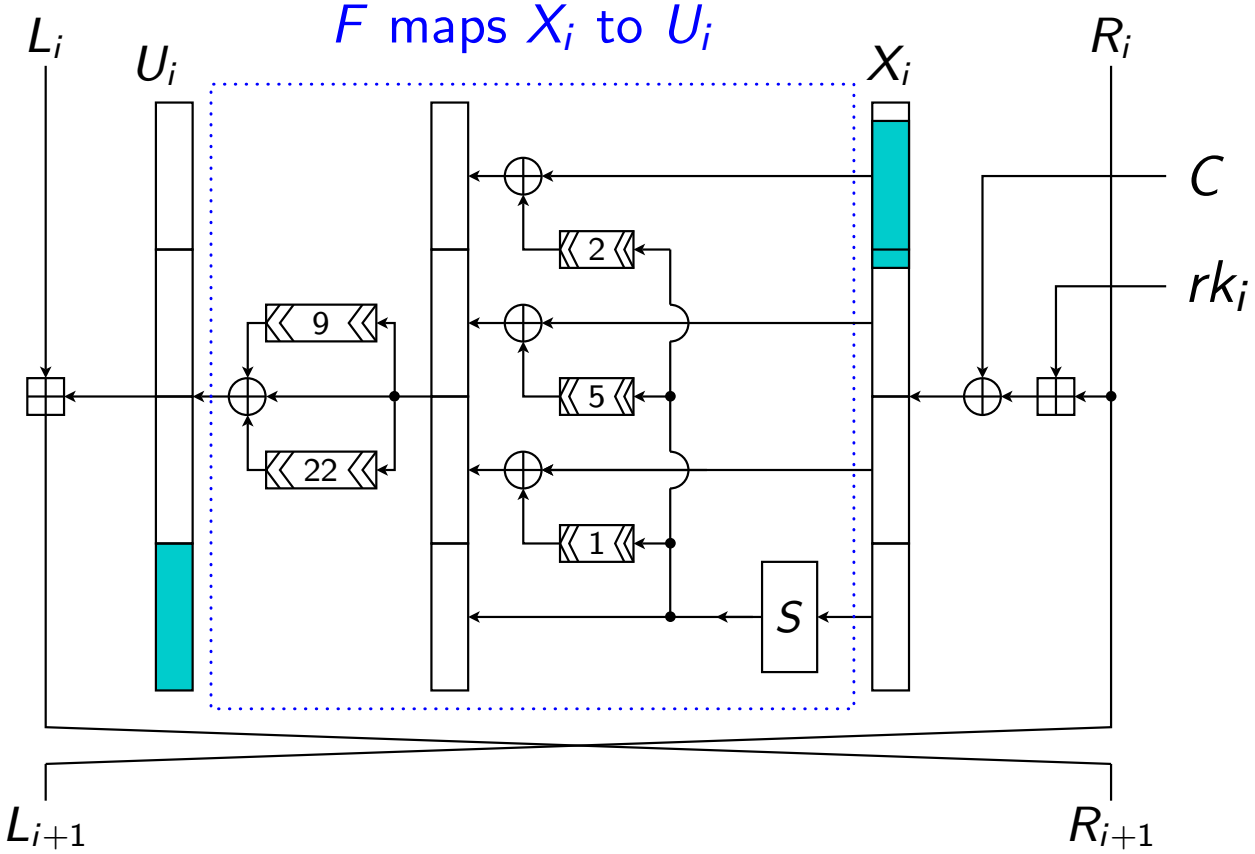
$$F(X \oplus (z \ll 23))_{0..7} = F(X)_{0..7} \oplus z$$



Generating plaintexts

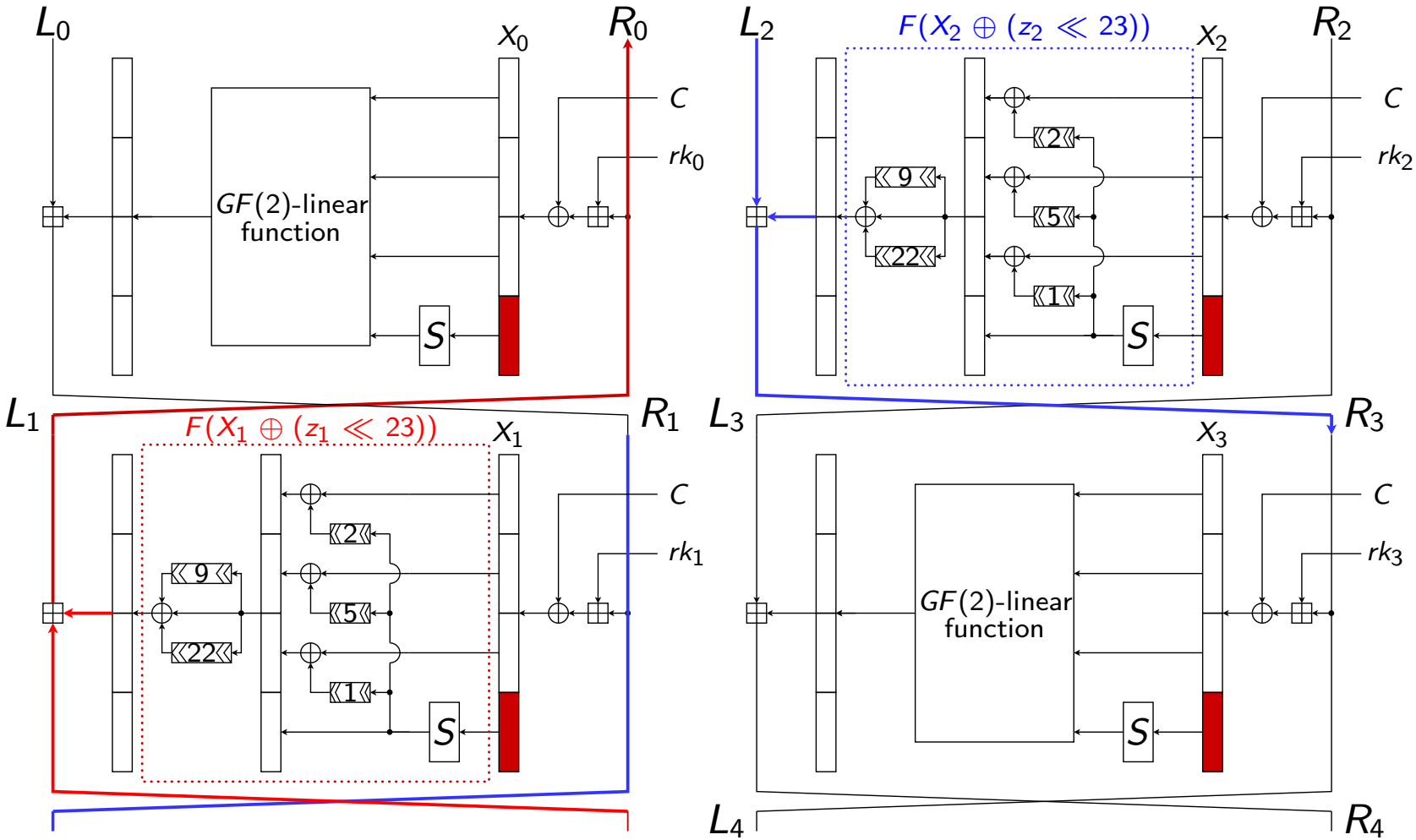
- For every 8-bit vector z holds

$$F(X \oplus (z \ll 23))_{0..7} = F(X)_{0..7} \oplus z$$



Generating plaintexts

- Find z_1 and z_2



Generating plaintexts

- Choose

$$L_2' = (X_1 \oplus (z_1 \lll 23) \oplus C) \boxminus rk_1$$

$$R_2' = (X_2 \oplus (z_2 \lll 23) \oplus C) \boxminus rk_2$$

- Decrypt 2 rounds, then the plaintext will satisfy the condition for 4 rounds.
- Complexity of generating a plaintext that also fits in round 5-7 is $\left(\frac{256}{3}\right)^3 = 2^{19}$ encryptions by trial-and-error.

Attacking a device

- Encrypt every plaintext
- Check whether ciphertext after 7 rounds is the expected one (three round test)
- If yes, 3 S-box entries are recovered
- Find plaintext which does not use unknown S-box entries in first 6 rounds and recover S-box entries of remaining rounds
- Complexity (in encryptions):
  - 2^{24} for the first 3 entries
  - 2^{20} for the remaining entries

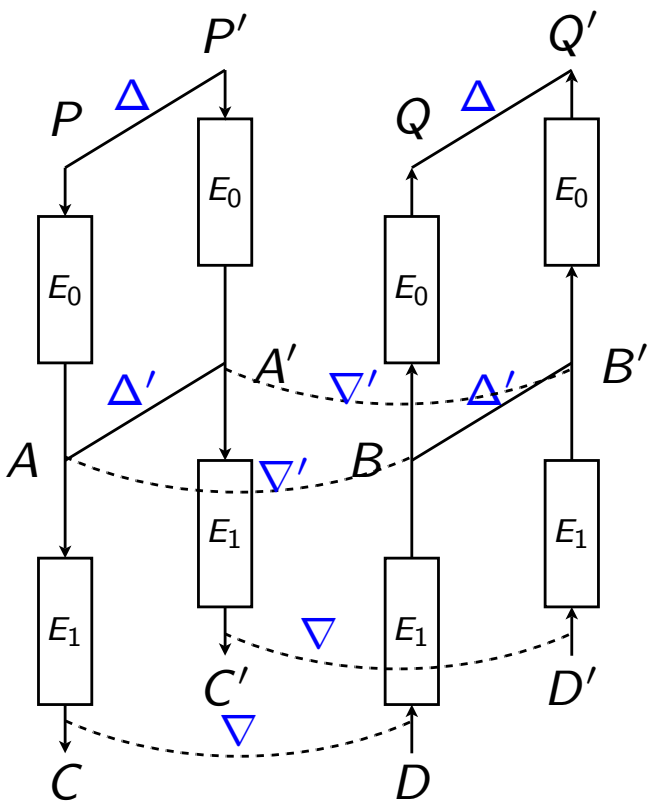
Outline of attack 2

- Find a characteristic for en- and decryption independent of the S-box with high probability
- Use this characteristic to build a boomerang
- Mount boomerang attack to recover parts of the first round key

Characteristics

- S-box and modular addition are nonlinear over $GF(2)$
- Differential behavior of the S-box may vary
- Search for characteristic in the linearized model of C2
- 5-round characteristic **independent of the S-box** with probability 2^{-12} (2^{-11})

Boomerang attack



- Assume S-box is known
- Use the 5-round characteristic to mount boomerang attack
- Boomerangs exist with average probability of $2^{-44.5}$
- All boomerangs follow the characteristic for the first round
- Use boomerang attack to recover 22 bits of the first round key
- Complexity: 2^{48} encryptions and $2^{44.5}$ chosen plaintext/ciphertext pairs

Examples for boomerangs

$$\Delta = 00020800\ \ 80200100 \rightarrow 80200100\ \ 00020800$$

S-box used	key (hex)	plaintext
AES	00 00 00 00 00 00 00 00	5707aec0 48a9c942
	00 30 20 08 00 20 28 00	0f42cd03 b7b5f077
	'c' 'r' 'y' 'p' 't' '0' '9'	b4b32db5 589913dc
C2 facsimile	00 00 00 00 00 00 00 00	3af32bac 960693e1
	ee 9b 7f 2b 7c 26 cd 00	69676fdc 339879d4
	'c' 'r' 'y' 'p' 't' '0' '9'	d6b44956 36771c9d

Key and S-box recovery attack (Attack 3)

- Combines the ideas of the first two attacks
- Complexity: $2^{53.5}$ encryptions

Conclusion

The three attacks and their complexities

	provided we can ...	recover	complexity
1.	set key + query device	S-box	2^{24}
2.	query device + know S-box	key	2^{48}
3.	query the device	S-box +key	$2^{53.5}$

Conclusion

The three attacks and their complexities

	provided we can ...	recover	complexity
1.	set key + query device	S-box	2^{24}
2.	query device + know S-box	key	2^{48}
3.	query the device	S-box +key	$2^{53.5}$

What is new?

- Recover the S-box when we are able to set the key
- Boomerang is independent of the S-box

Conclusion

The three attacks and their complexities

	provided we can ...	recover	complexity
1.	set key + query device	S-box	2^{24}
2.	query device + know S-box	key	2^{48}
3.	query the device	S-box +key	$2^{53.5}$

What is new?

- Recover the S-box when we are able to set the key
- Boomerang is independent of the S-box

Thank you!