Reducing 2^{1740} to 2^{54} or how to break C2

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

Department of Mathematics
Technical Univeristy of Denmark

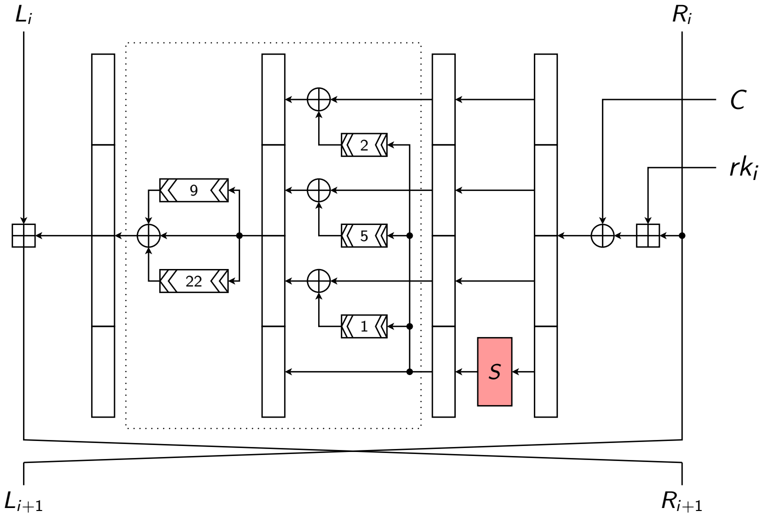
FSE 2009 rump session, 24 February 2009

C2: a block cipher with a twist

- 64-bit block cipher with 56-bit key
- Designed by 4C Entity (IBM, Intel, Matsushita and Toshiba)
- Used in CPRM/CPPM Digital Rights Management scheme
- DVD-Audio, DRM-restricted SD-cards

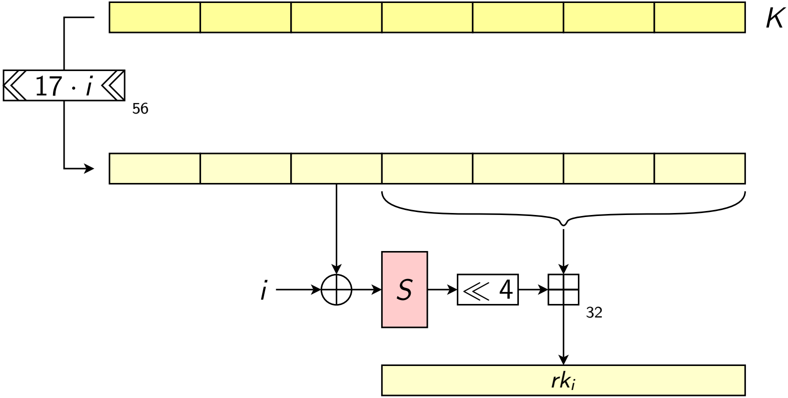
C2: round function

- 10 Feistel rounds



C2: key scheduling

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



The twist

- 8×8 S-box is kept secret
- Equivalent to ≥ 1684 secret bits $+$ 56 bits of the key
- Possible attack scenarios:

	provided we	recover
1.	can set the key, query the device	S-box
2.	know the S-box, can query the device	key
3.	can query the device	S-box $+$ key

Chosen key S-box recovery

- There are master keys that generate only three distinct inputs to the S-box in the key scheduling.
- Generate plaintexts using only those three inputs to the S-box in the first 7 rounds
- Use an S-box-independent check in rounds 8 – 10 to see if the state after 7th round matches the device's ciphertext
- After 2^{24} guesses we recover 3 S-box entries, the rest is easy
- Total complexity: $\approx 2^{24}$ queries

Key and key+S-box recovery attacks

- We found 5-round differential characteristic with probability $\approx 2^{-11}$
- Characteristic is independent of the S-box
- Mount boomerang attack (boomerang probability $\approx 2^{-44}$ on average)
- Similar ideas to recover the S-box

Summary

- Three types of attacks on secret S-box based cipher C2

	provided we	recover	complexity
1.	can set the key, query the device	S-box	2^{24}
2.	know the S-box, query the device	key	2^{48}
3.	query the device	S-box + key	2^{54}

- All the details in a forthcoming paper (currently under review)