Complementing CLEFIA-128

Ivica Nikolić, Josef Pierpzyk, Sareh Emami, San Ling, Huaxiong Wang

Nanyang Technological University, Singapore
Macquarie University, Sydney

12 March 2013

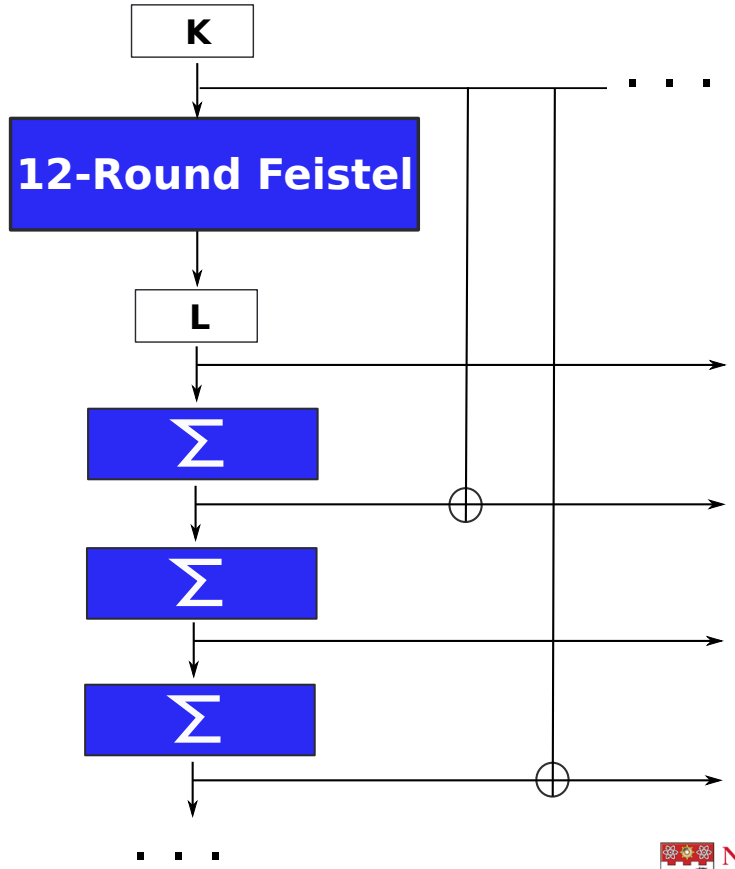
NANYANG TECHNOLOGICAL UNIVERSITY

Specifications

CLEFIA-128:

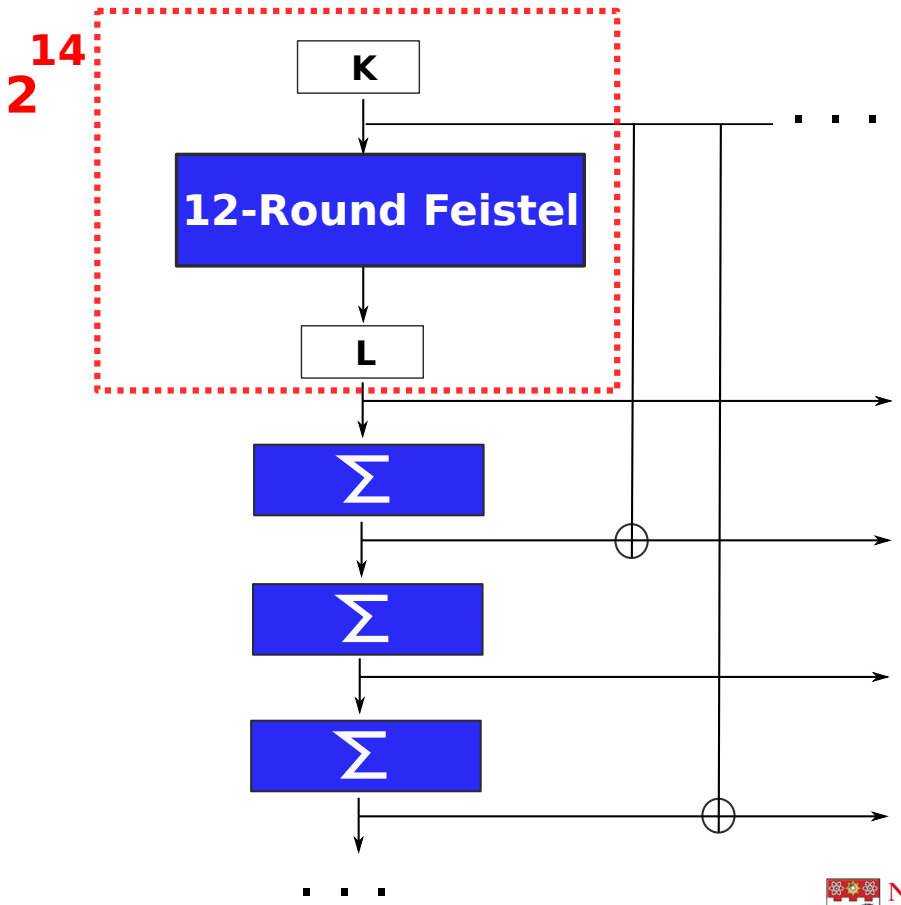
- four-branch generalized Feistel cipher
- 128-bit key
- 18 rounds
- Feistel round = XOR of subkey + transformation

Key Schedule



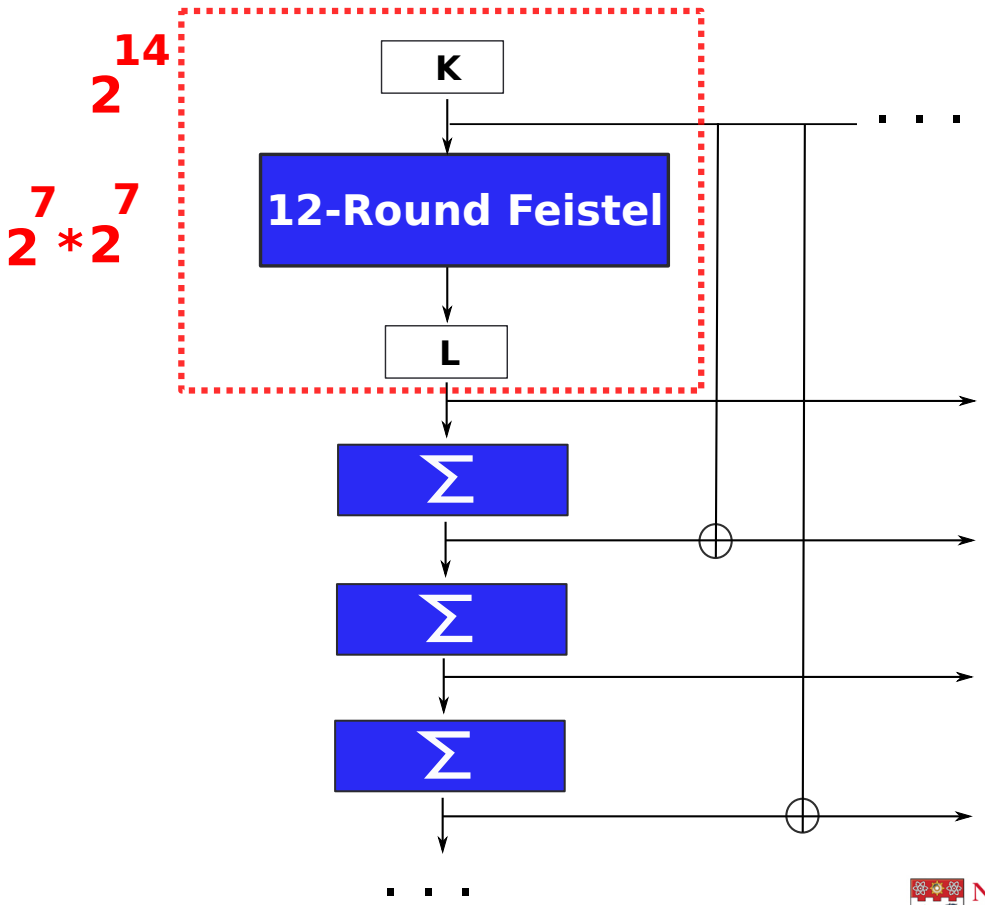
Key Schedule

- 2^{14} good $(\Delta K, \Delta L)$
-
-
-



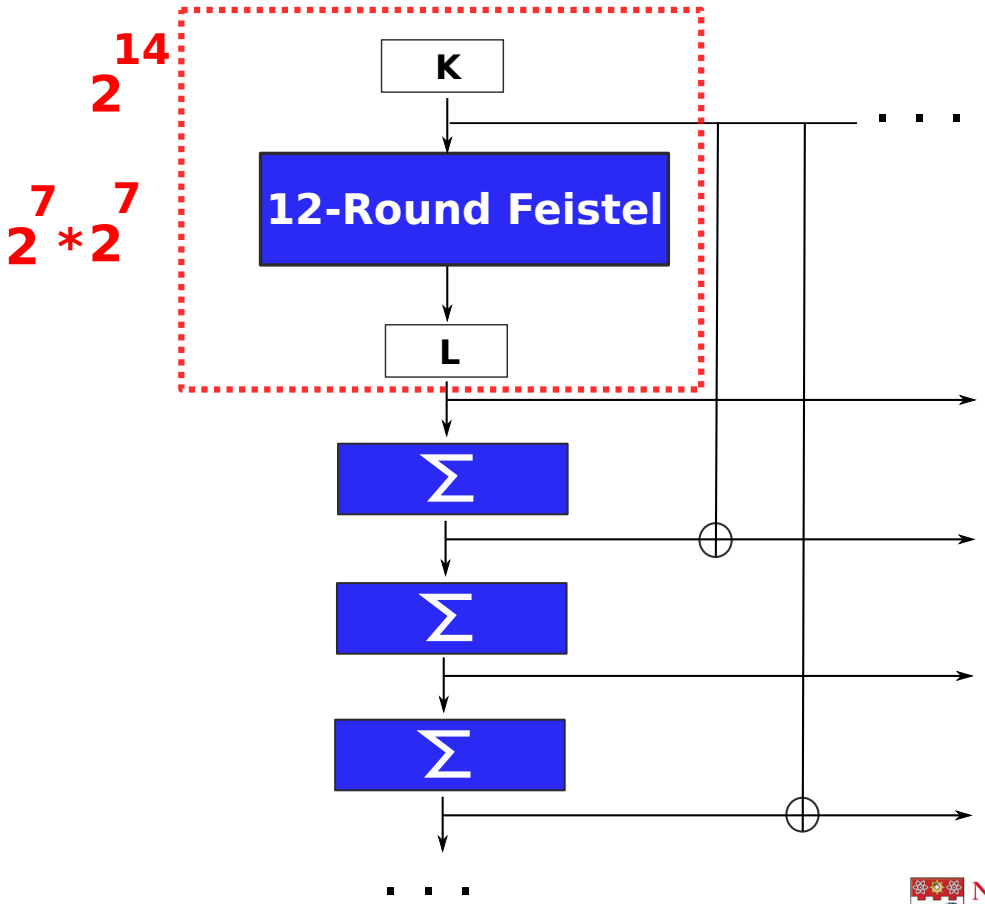
Key Schedule

- 2^{14} good $(\Delta K, \Delta L)$
- **Can be split on** $2^7 \cdot 2^7$
-
-



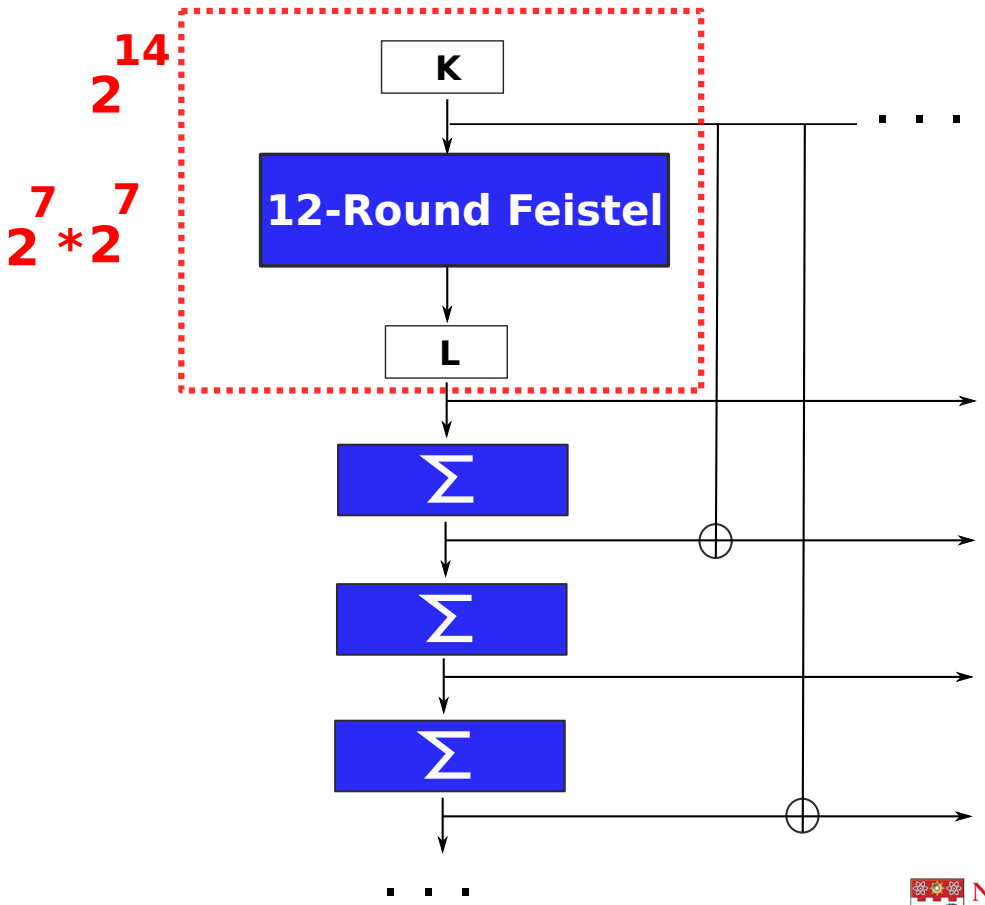
Key Schedule

- 2^{14} good $(\Delta K, \Delta L)$
- **Can be split on** $2^7 \cdot 2^7$
- Two structures of 2^7 (plaintext,keys)
-



Key Schedule

- 2^{14} good $(\Delta K, \Delta L)$
- **Can be split on** $2^7 \cdot 2^7$
- Two structures of 2^7 (plaintext,keys)
- Check on collisions = save factor 2^7



Results

Full-round CLEFIA-128

- Weak-key class of 2^{14} keys
- Related-key distinguisher with $2^{122.5}$ encryptions, and 2^{122} data

Similar results for CLEFIA-256