The ZUC-256 Stream Cipher

Bin Zhang

martin_zhangbin@hotmail.com

Outline

256-bit Symmetric-key Algorithms in 5G & Post-quantum Era

ETSI/SAGE 3GPP

- SNOW 3G in 128-EEA1 & 128-EIA1 → SNOW 3G-256
- AES in 128-EEA2 & 128-EIA2 → AES-256
- ZUC in 128-EEA3 & 128-EIA3 → ZUC-256

ZUC-256

- Configuration: a 256-bit secret key and a 184-bit IV.
- Confidentiality: for each key/IV pair, the frame consists of 20000 to 2^{32} bits keystream.
- Integrity: generate $32/64/128$-bit authentication tags, but could support up to 256-bit tag if needed.

ZUC-256

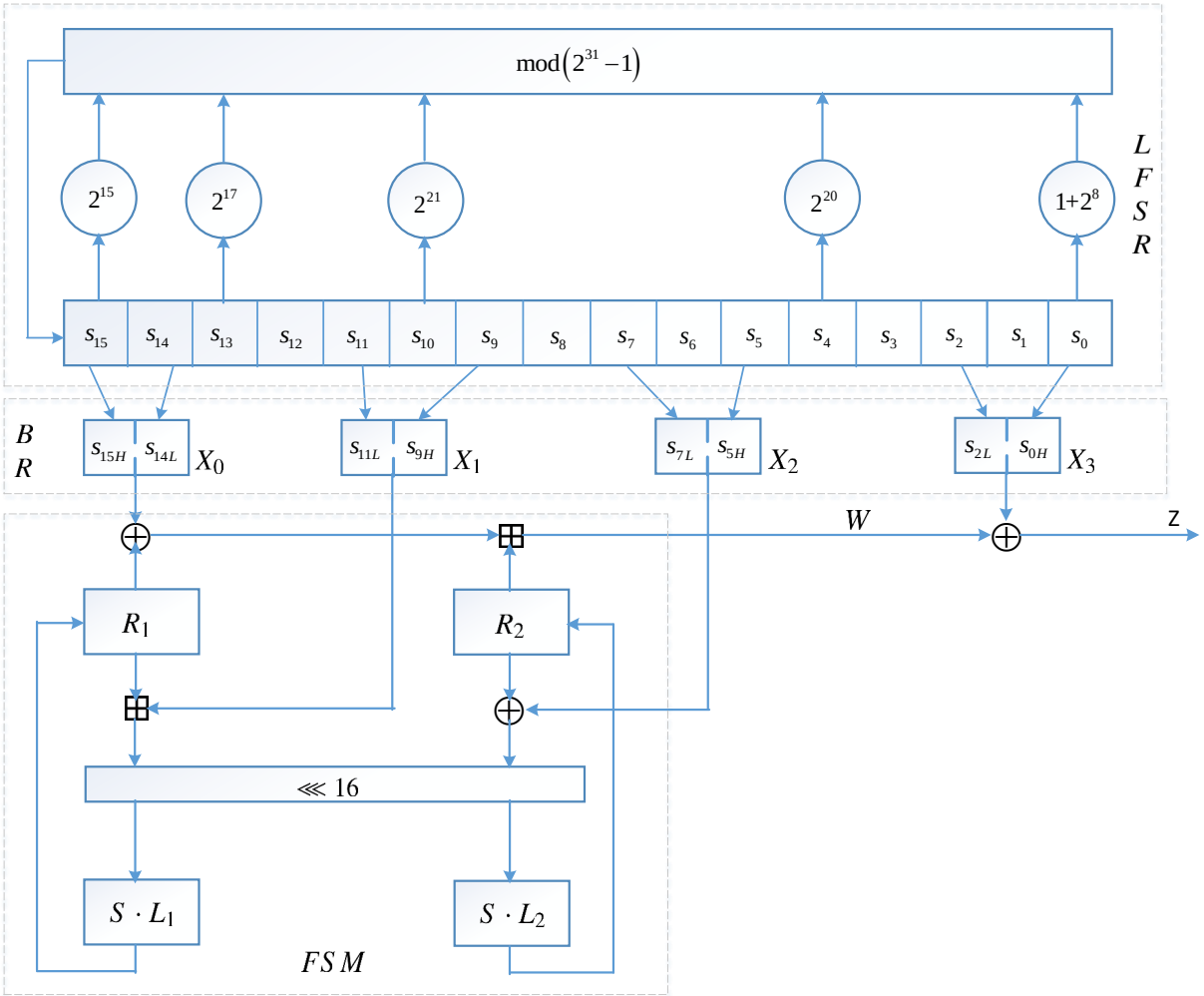

Figure: The keystream generation of ZUC-256

ZUC-256

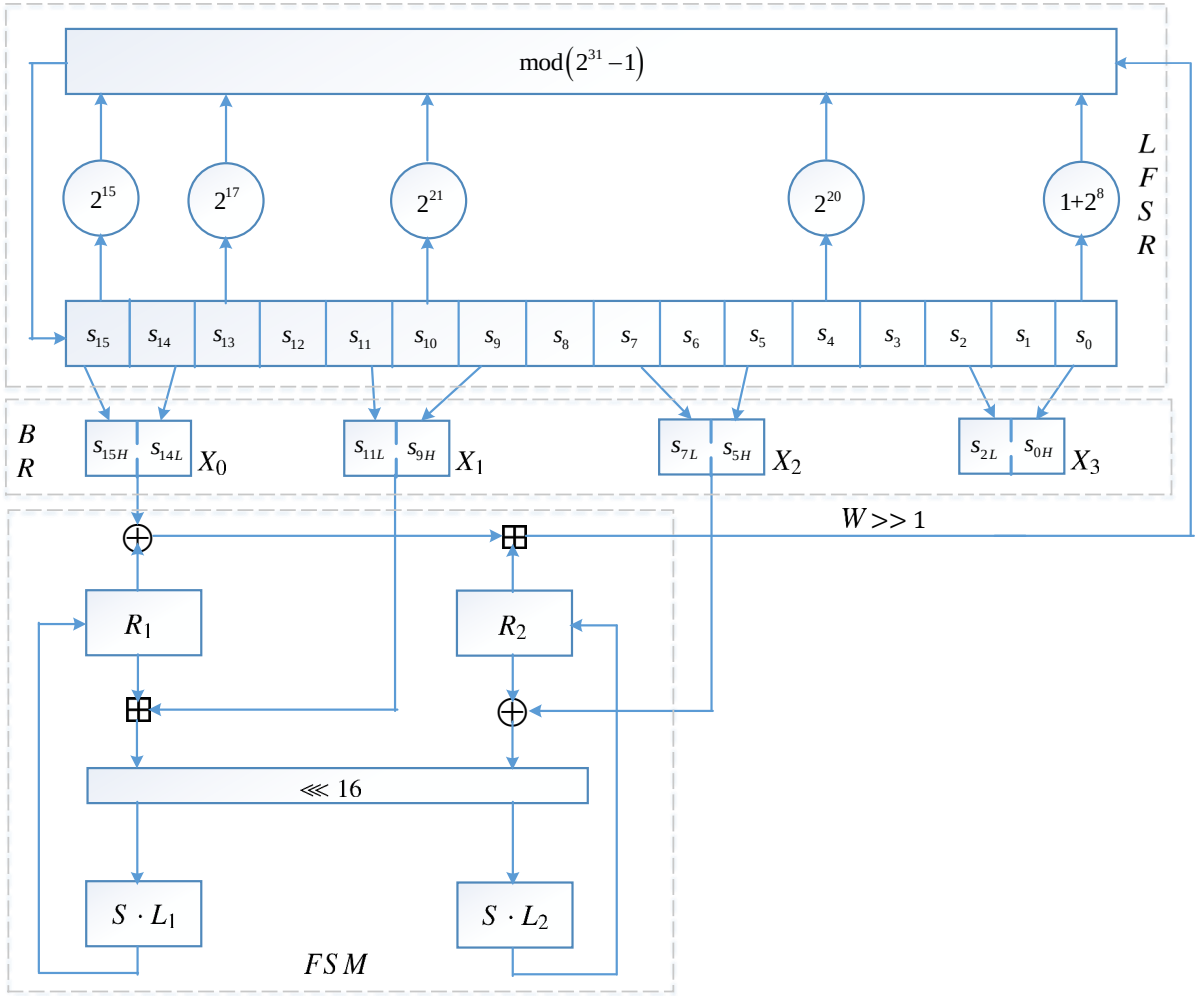

Figure: The initialization phase of ZUC-256

ZUC-256 & ZUC-128

- ZUC-256 differs from ZUC-128 only in the initialization phase and in the message authentication codes generation phase.
- http://dacas.cn/thread.aspx?ID=3621
- http://www.is.cas.cn/ztzl2016/zouchongzhi/index.html

Cryptanalysis Awards

- The best cryptanalysis paper on ZUC-256 will be awarded at the ZUC-256 conference.

- The best software/hardware implementation of ZUC-256 will also be awarded at the ZUC-256 conference.

→ martin_zhangbin@hotmail.com

ZUC-256 Conference Time

- The 6th of July, 2018 at Beijing, China