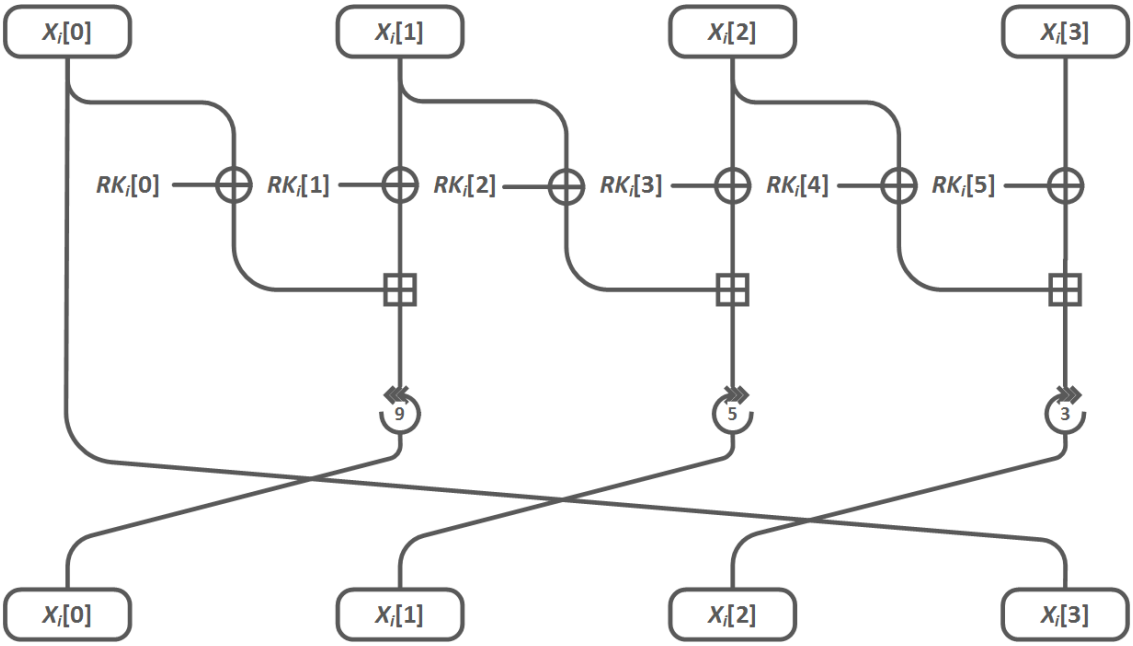
Cryptanalysing LEA, a lightweight ARX-C Cipher



ARX primitives are cryptographic constructions that only use some combinations of Addition, Rotation and XOR operations. ARX constructions that also involve injecting constants into the internal state by the means of the same operations are termed as ARX-C primitives. Rotational cryptanalysis was introduced as a technique to efficiently cryptanalyse ARX constructions. However, ARX-C constructions prove to be quite resistant to this technique. To adress this issue, rotational-XOR cryptanalysis was introduced. This technique uses rotational-XOR pairs instead of only rotational pairs to cryptanalyse ARX-C ciphers where the constant was injected to the internal state by the means of XOR operation.

The goal of this thesis is as follows. The student will learn the feasibility of using rotational pairs as well as rotational-XOR pair to attack ARX-C ciphers, and then will use that to cryptanalyse LEA, a lightweight ARX-C cipher that has not yet been analysed in the context of rotational cryptanalysis. Students interested in this thesis are requested to send an email to Arka Debnath to confirm that they have the required mathematical background.

Practicalities

Promotor:	Prof. Bart Preneel
Daily supervisor:	Arka Debnath arka.debnath@esat.kuleuven.be office 01.34
Nature of the work:	30% literature, 70% theoretical work
Number of students:	1

 © 2026 – 2027 COSIC