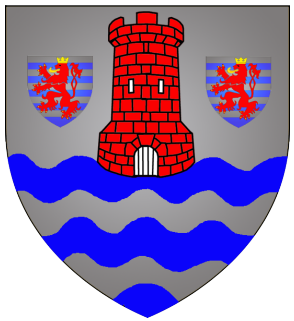
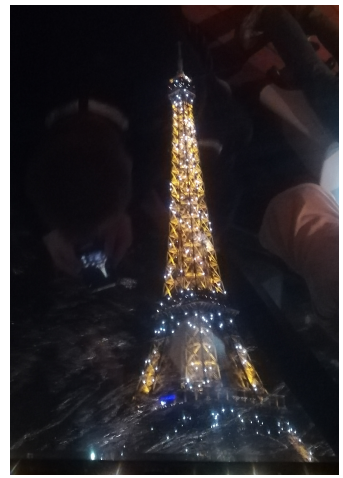
SPARKLE Permutations

Christof Beierle[1], Alex Biryukov[1], Luan Cardoso dos Santos[1], Johann Großschädl[1], Léo Perrin[2], Aleksei Udovenko[1], Vesselin Velichkov[3], Qingju Wang[1]

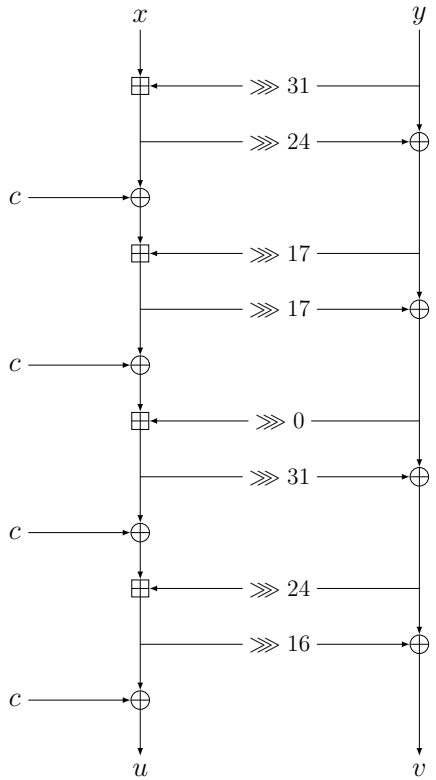
[1]SnT and CSC, University of Luxembourg, Luxembourg
[2]Inria, SECRET, France
[3]University of Edinburgh, UK

FSE'19 Rump Session, Paris



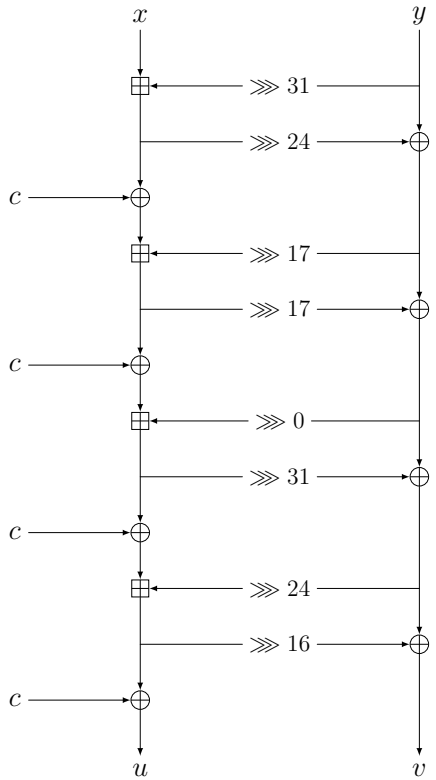


SPARX-like Permutations

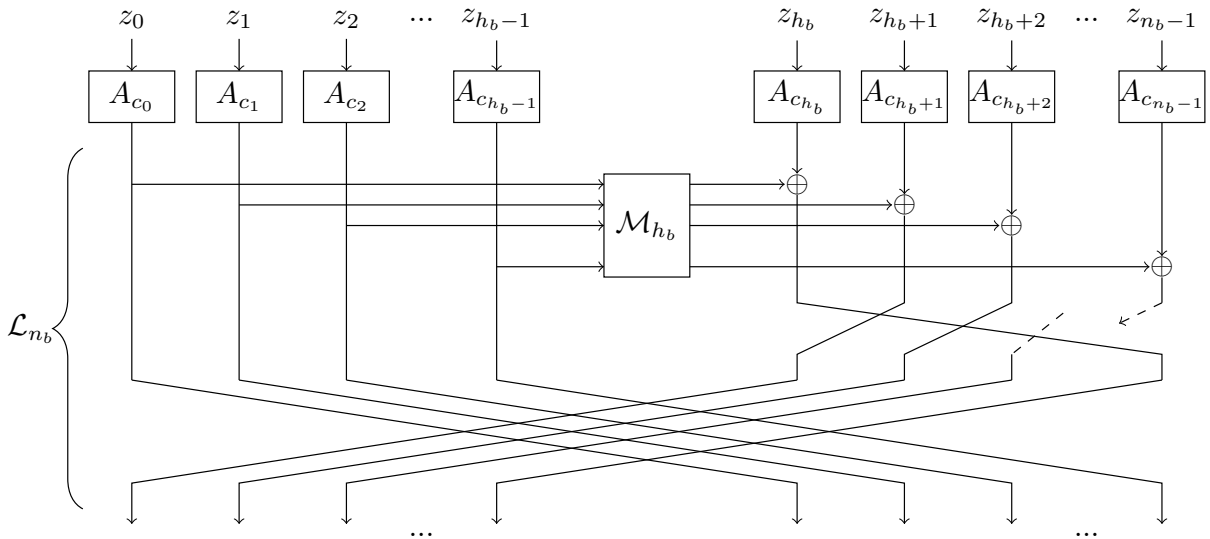


ARX-box: a 64-bit S-box

SPARX-like Permutations



ARX-box: a 64-bit S-box



Step structure: an **SPN** round!

Two versions: slim for absorbing, big for squeezing.

SPARKLE NIST submission

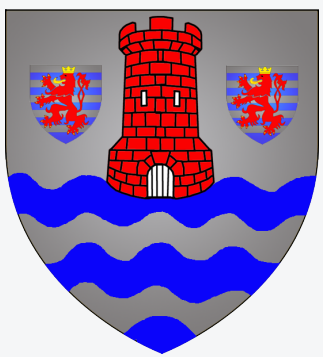
Overall goal: Fast Software Encryption!

Instances

SPARKLE256 SPARKLE384 SPARKLE512

Hashing: **ESCH**

Efficient,
Sponge-based, and
Cheap **H**ashing



AEAD: **SCHWAEMM**

Sponge-based **C**ipher for **H**ardened but **W**eightless **A**uthenticated **E**ncryption on **M**any **M**icrocontrollers

More informations

Mailing list `sparklegrupp@googlegroups.com`

Website `https://www.cryptolux.org/index.php/Sparkle`