Many GIFT, is it Xmas?

Subhadeep Banik[1,2] Sumit Kumar Pandey[1]
Thomas Peyrin[1] Yu Sasaki[3]
Siang Meng Sim[1] Yosuke Todo[3]

1. Nanyang Technological University, Singapore
2. École Polytechnique Fédérale de Lausanne, Switzerland
3. NTT Secure Platform Laboratories, Japan

CHES2017, Rump Session

GIFT-64

GIFT-64 is a new 64-bit lightweight block cipher (presenting tomorrow), improving over PRESENT, more secure and better performances.

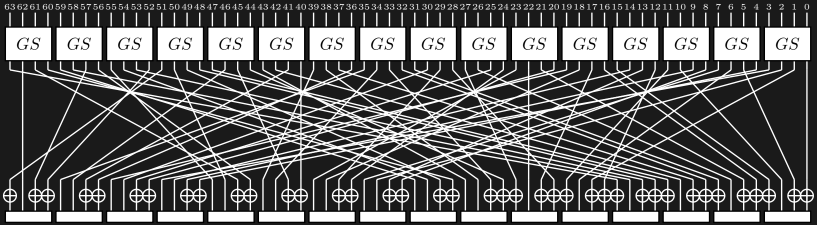
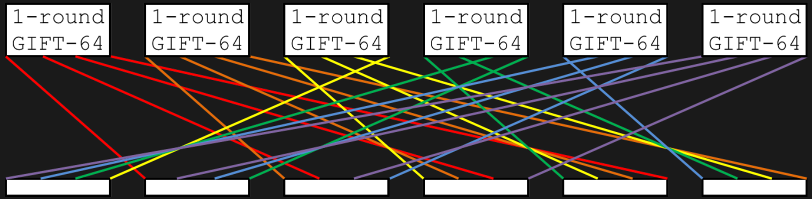


Figure: 1 Round of GIFT-64.

Larger permutation from GIFT-64

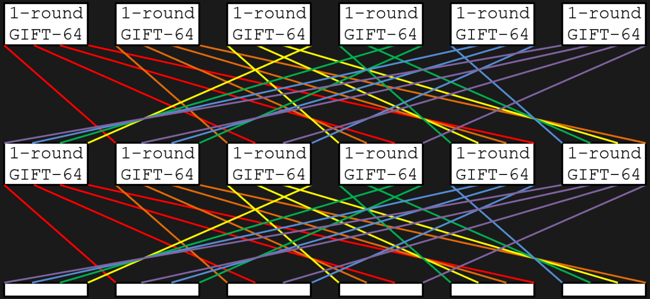
Easily build a larger permutation, say 384-bit, from GIFT-64:

- exclude the AddRoundKey,
- apply 6 blocks of GIFT-64 in parallel,
- after every 1-round GIFT-64, shuffle the bits to other blocks.



Each line contains 16 bits.

Name?



There are many GIFT in this network, let's call it...

Xmas

Xmas and Gimli

Quick comparison with Gimli, a new 384-bit permutation

Implementation:
Round based implementation of Xmas requires
576 XOR/XNOR, 384 AND/OR (excluding add constants)

Round based implementation of Gimli requires
740 XOR, 360 AND/OR (excluding add constants)

Security:

	Differential	**Rounds**							
	Bounds	3	4	5	6	7	8	9	10
Xmas	active Sboxes	3	5	7	10	13	17	22	≥ 27
	prob, $-\log_2(\cdot)$	7	13	19	27	34	45	58	≈ 70
Gimli	prob, $-\log_2(\cdot)$	2	6	12	22	36	52		

Xmas Gimli?

Thank you. :)