

# LIGHTWEIGHT APPROACHES IN BLOCK CRYPTOGRAPHY

Presentación examen final

Metodologia de la Investigación en Computación  
Fernando Ramirez Arredondo

CS401

Universidad Católica San Pablo

13 de diciembre de 2023

# Taxonomia

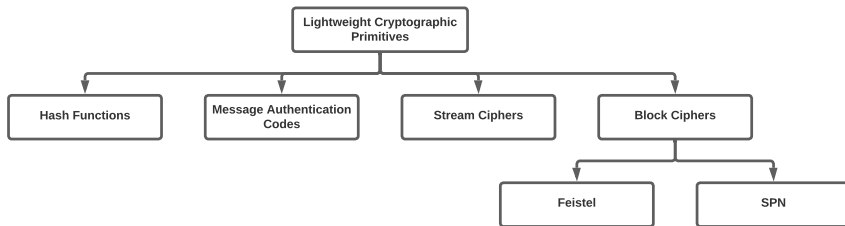


Figura: Taxonomia del survey.

## Lightweight Block Ciphers

Algorithm	Key size	Block size	Structure	N. of rounds
AES-128 (Daemen and Rijmen, 1999) [1] [2]	128	128	SPN	10
mCrypton (Lim and Korkishko, 2005) [3]	64/96/128	64	SPN	12
PRESENT (Bogdanov et al., 2007) [4]	80/128	64	SPN	31
LED (Guo et al., 2011) [5]	64/128	64	SPN	32/48
Hummingbird-2 (Engels et al., 2012) [6]	256	16	SPN	4
PRINCE (Borghoff et al., 2012) [7]	128	64	SPN	12
GIFT (Banik et al., 2017) [8]	128	64/128	SPN	28/40
DULBC (Yang et al., 2022) [9]	64/128	64	SPN	25/30
HIGHT (Hong et al., 2006) [10]	128	64	Feistel	32
DESL (Leander et al., 2007) [11]	54	64	Feistel	16
LBlock (Wu and Zhang, 2011) [12]	80	64	Feistel	32
TWINE (Suzaki et al., 2012) [13]	80-128	64	Feistel	36
GOST 28147-89 (Courtois, 2012) [14]	256	64	Feistel	32
QTL (Li et al., 2016) [15]	64/128	64	Feistel	16/20
SLIM (Aboushosha et al., 2020) [16]	80	32	Feistel	32
SHADOW (Guo et al., 2021) [17]	64/128	32/64	Feistel	16/32

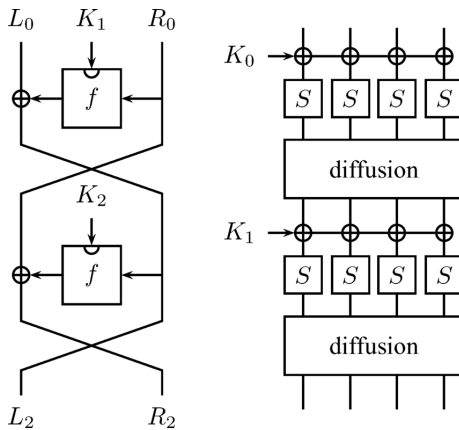


Figura: Feistel Network [18] y SPN [19].

# SLIM

## SLIM

- 80-bit key.
- 32-bit block.
- 32 rounds.

- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus P(S(K_i \oplus R_{i-1}))$

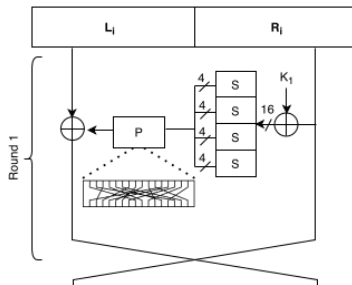
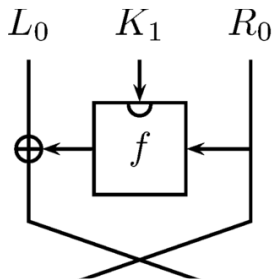


Figura: Comparación de round functions, Feistel Network genérica y SLIM.

# SLIM

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Cuadro: S-box de SLIM

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
P(x)	7	D	1	8	B	E	2	5	4	A	F	0	3	6	9	C

Cuadro: P-box de SLIM

# GIFT

## GIFT-64

- 128-bit key.
- 64-bit block.
- 28 rounds.

## GIFT-128

- 128-bit key.
- 128-bit block.
- 40 rounds.

Se coloca cada bit del plaintext en un bloque.

0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15
16	20	24	28	17	21	25	29	18	22	26	30	19	23	27	31
32	36	40	44	33	37	41	45	34	38	42	46	35	39	43	47
48	52	56	60	49	53	57	61	50	54	58	62	51	55	59	63

Figura: Posición de los bits. Los sectores 0,1,2,3 están en rojo, amarillo, verde y azul respectivamente.



# GIFT-64

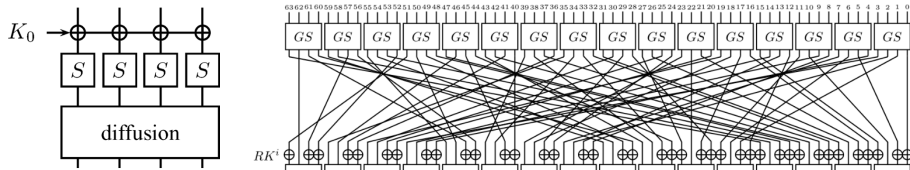


Figura: Comparación de round functions, SPN generica y GIFT.

# GIFT-64

16 S-boxes se implementan en paralelo en forma de bitslice.

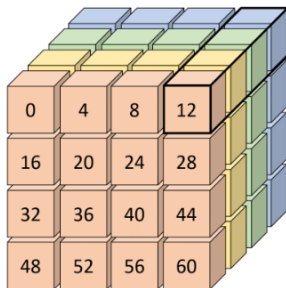


Figura: Representación cúbica del estado principal de GIFT-64. El cuboide negro es donde se implementa un S-box.

# GIFT-64

La permutación de bits (P-box) se implementa de la siguiente manera:

- Sacar la transpuesta a cada sector.
- Sector 0: intercambie la fila 1 con la 3.
- Sector 1: intercambie la fila 0 con 1 y intercambie la fila 2 con 3.
- Sector 2: intercambie la fila 0 con 2.
- Sector 3: intercambie la fila 0 con 3 y intercambie la fila 1 con 2.

0	16	32	48
4	20	36	52
8	24	40	56
12	28	44	60

1	17	33	49
5	21	37	53
9	25	41	57
13	29	45	61

2	18	34	50
6	22	38	54
10	26	42	58
14	30	46	62

3	19	35	51
7	23	39	55
11	27	43	59
15	31	47	63

Figura: Los cortes después de la transposición. Los cuadros negros son las filas que serán intercambiadas.

# Conclusiones




## Feistel Network

- Simpleza.
- Descifrado.
- Seguridad.
- Mucha simpleza!




## Substitution-Permutation Network

- Libertad.
  - Diseño.
  - Implementación: paralelismo, hardware/software.
- Mucha libertad!

# References I

-  M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, “Strong authentication for rfid systems using the aes algorithm,” in *Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings 6*. Springer, 2004, pp. 357–370.
-  J. Daemen and V. Rijmen, “Aes proposal: Rijndael,” 1999.
-  C. H. Lim and T. Korkishko, “mcrypton—a lightweight block cipher for security of low-cost rfid tags and sensors,” in *International workshop on information security applications*. Springer, 2005, pp. 243–258.

# References II

-  A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsøe, “Present: An ultra-lightweight block cipher,” in *Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9*. Springer, 2007, pp. 450–466.
-  J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, “The led block cipher,” in *Cryptographic Hardware and Embedded Systems-CHES 2011: 13th International Workshop, Nara, Japan, September 28–October 1, 2011. Proceedings 13*. Springer, 2011, pp. 326–341.
-  D. Engels, M.-J. O. Saarinen, P. Schweitzer, and E. M. Smith, “The hummingbird-2 lightweight authenticated encryption algorithm,” in *RFID. Security and Privacy: 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26-28, 2011, Revised Selected Papers 7*. Springer, 2012, pp. 19–31.

# References III






J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger *et al.*, “Prince—a low-latency block cipher for pervasive computing applications,” in *Advances in Cryptology—ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings 18*. Springer, 2012, pp. 208–225.







S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. M. Sim, and Y. Todo, “Gift: A small present: Towards reaching the limit of lightweight encryption,” in *Cryptographic Hardware and Embedded Systems—CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*. Springer, 2017, pp. 321–345.

# References IV



-  J. Yang, L. Li, Y. Guo, and X. Huang, “Dulbc: A dynamic ultra-lightweight block cipher with high-throughput,” *Integration*, vol. 87, pp. 221–230, 2022.
-  D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong *et al.*, “Hight: A new block cipher suitable for low-resource device,” in *Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8*. Springer, 2006, pp. 46–59.
-  G. Leander, C. Paar, A. Poschmann, and K. Schramm, “New lightweight des variants,” in *Fast Software Encryption: 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers 14*. Springer, 2007, pp. 196–210.



# References V

-  W. Wu and L. Zhang, “Lblock: a lightweight block cipher,” in *Applied Cryptography and Network Security: 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10, 2011. Proceedings 9*. Springer, 2011, pp. 327–344.
-  T. Suzaki, K. Minematsu, S. Morioka, and E. Kobayashi, “+: a lightweight block cipher for multiple platforms,” in *International Conference on Selected Areas in Cryptography*. Springer, 2012, pp. 339–354.
-  N. T. Courtois, “Security evaluation of gost 28147-89 in view of international standardisation,” *Cryptologia*, vol. 36, no. 1, pp. 2–13, 2012.
-  L. Li, B. Liu, and H. Wang, “Qtl: a new ultra-lightweight block cipher,” *Microprocessors and Microsystems*, vol. 45, pp. 45–55, 2016.

# References VI

-  B. Aboushousha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed, and M. M. Dessouky, "Slim: A lightweight block cipher for internet of health things," *IEEE Access*, vol. 8, pp. 203 747–203 757, 2020.
-  Y. Guo, L. Li, and B. Liu, "Shadow: A lightweight block cipher for iot nodes," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 13 014–13 023, 2021.
-  V. Nachev, J. Patarin, and E. Volte, "Feistel ciphers," *Cham: Springer International Publishing*, 2017.
-  H. M. Heys and S. E. Tavares, "Substitution-permutation networks resistant to differential and linear cryptanalysis," *Journal of cryptography*, vol. 9, no. 1, pp. 1–19, 1996.