Securing Data in Low-Resource Systems: Lightweight Block Cryptography Strategies

Presentación examen parcial

Proyecto de Final de Carrera I

Fernando Ramirez Arredondo

CCOMP8-1
Universidad Católica San Pablo

15 de mayo de 2024

Introducción

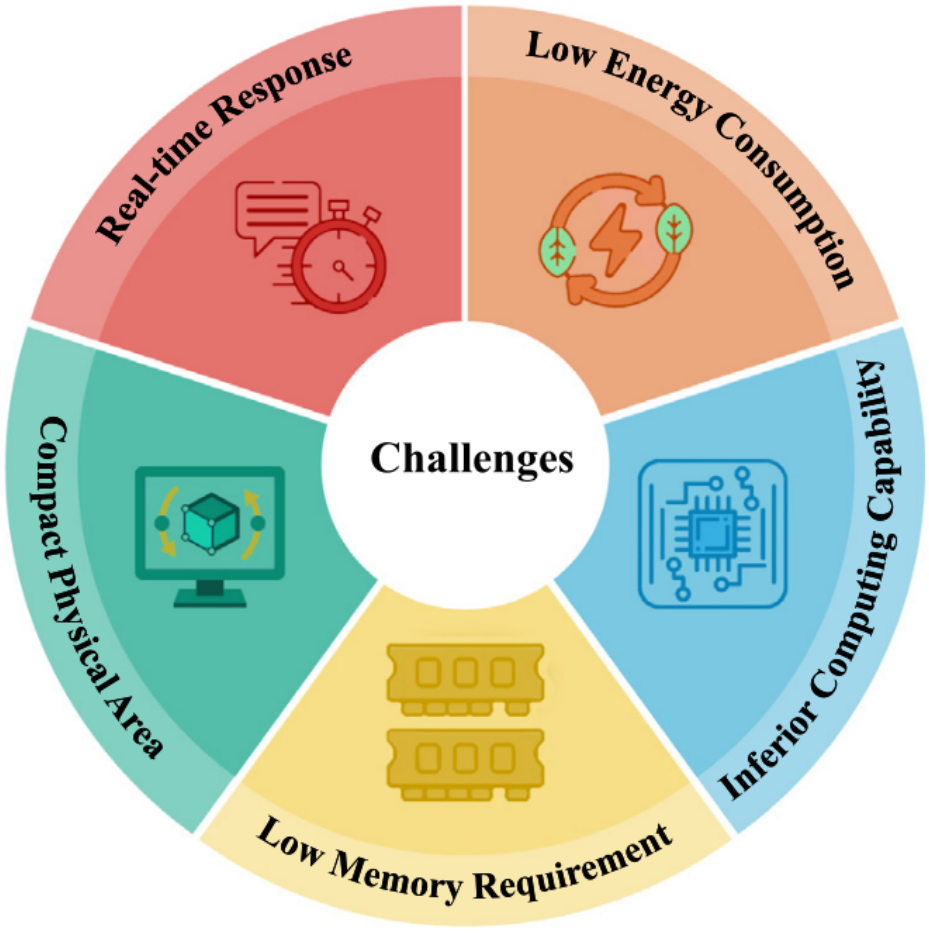


Figura: Desafíos clave con la criptografía convencional en dispositivos con recursos limitados [1].

Lightweight Block Ciphers

Algorithm	Key size	Block size	N. of rounds	Structure
DULBC (Yang et al., 2022) [2]	80/128	64	25/30	SPN
GIFT (Yasmin and Gupta, 2023) [3] [4]	128	64/128	28/40	SPN
IVLBC (Huang et al., 2023) [5]	80/128	64	29	SPN
LBC-IoT (Ramadan et al., 2021) [6]	80	32	32	Feistel
SAND (Chen et al., 2021) [7]	128	64/128	48/54	Feistel
LBCCS (Zhu et al., 2022) [8]	128	128	20	Feistel
SCENERY (Feng and Li et al., 2022) [9]	80	64	28	Feistel

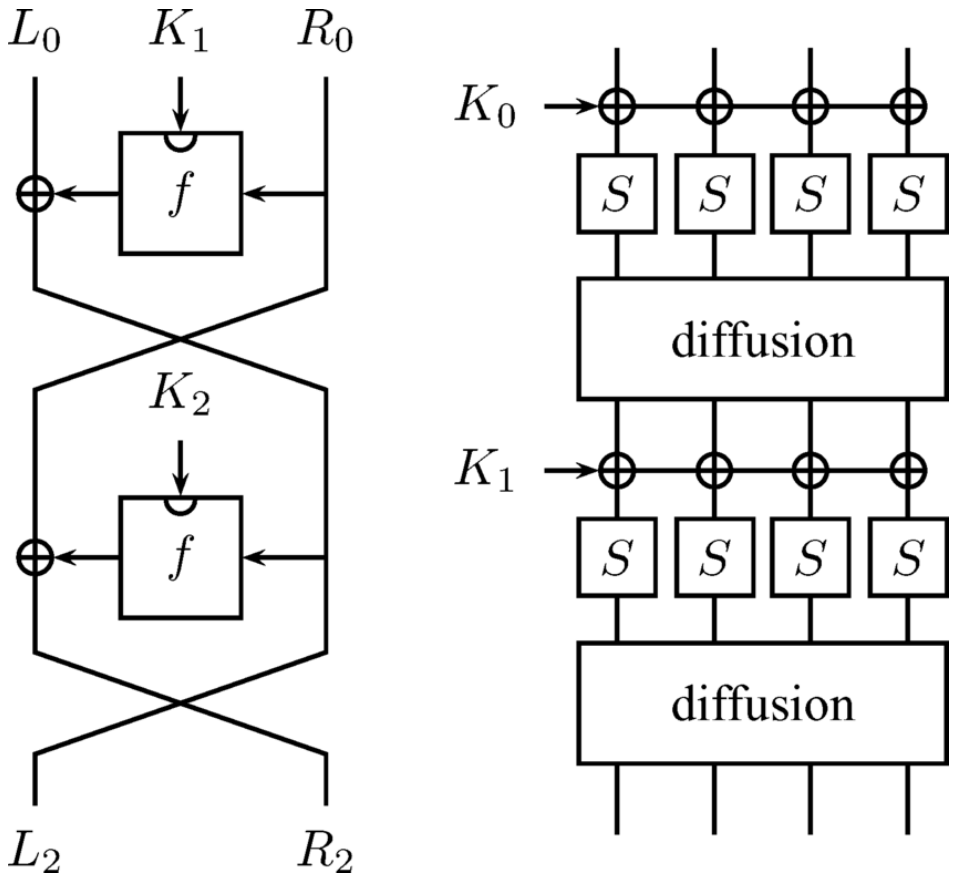


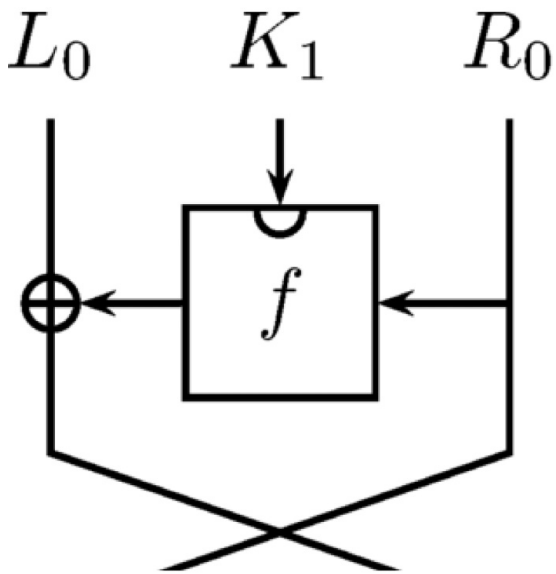
Figura: Generalizacion de una Feistel network [10] y Substitution-permutation network [11].

SAND

SAND

SAND-64 y SAND-128

- operaciones AND-RX = ligero.
- Synthetic s-box = seguro.
- 128-bit key, 64/128-bit block, 48/54 rounds.



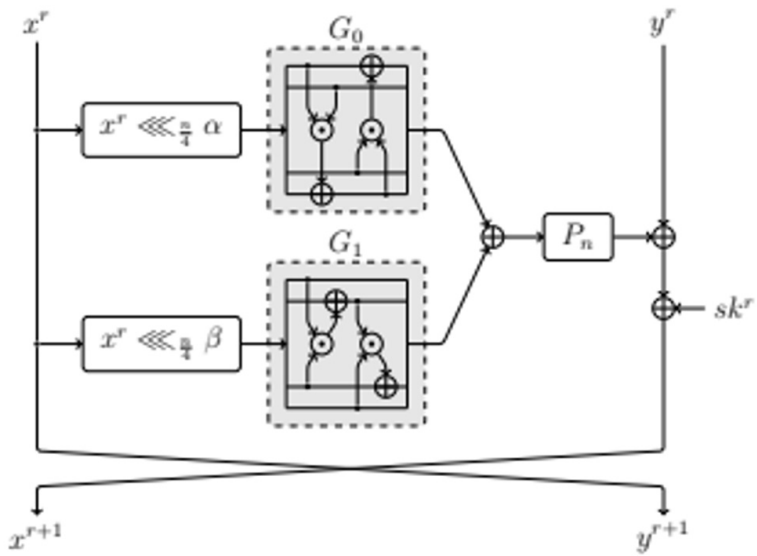


Figura: Comparación de round functions, Feistel network genérica y SAND [7].

(3) Non-linear Functions G_0 and G_1

Let the n-bit variable x be the input value of G_0 and G_1, which is regarded as the concatenation of four $\frac{n}{4}$-bit words $x\{3\}\|x\{2\}\|x\{1\}\|x\{0\}$. Let $y = y\{3\}\|y\{2\}\|y\{1\}\|y\{0\}$ denote the output value. For G_0, we have

$$
\begin{aligned}
y\{0\} &= x\{3\} \odot x\{2\} \oplus x\{0\}, \\
y\{3\} &= y\{0\} \odot x\{1\} \oplus x\{3\}, \\
y\{2\} &= x\{2\}, \\
y\{1\} &= x\{1\}.
\end{aligned}
$$

As to the function G_1, the output is calculated as

$$
\begin{aligned}
y\{2\} &= x\{3\} \odot x\{1\} \oplus x\{2\}, \\
y\{1\} &= y\{2\} \odot x\{0\} \oplus x\{1\}, \\
y\{3\} &= x\{3\}, \\
y\{0\} &= x\{0\}.
\end{aligned}
$$

Figura: Definición formal de las funciones G de SAND [7].

SAND

x	0	1	2	3	4	5	6	7	8	9	A	B	C
$N_0(x)$	0	1	2	B	4	5	6	F	8	9	A	3	D
$N_1(x)$	0	1	2	3	4	7	6	5	8	9	E	D	C
Ssb(x)	00	11	22	B3	44	57	66	F5	88	99	AE	3D	DC

Cuadro: Synthetic S-box de SAND-128

SAND

x	0	1	2	3	4	5	6	7
P(x)	7	4	1	6	3	0	5	2

Cuadro: P-box de SAND-64

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

Cuadro: P-box de SAND-128

GIFT

GIFT

GIFT-64 y GIFT-128

- Feistel = ligero.
- Bitslice substitution = seguro.
- Involutive permutation = más seguro!
- 128-bit key, 64/128-bit block, 28/40 rounds.

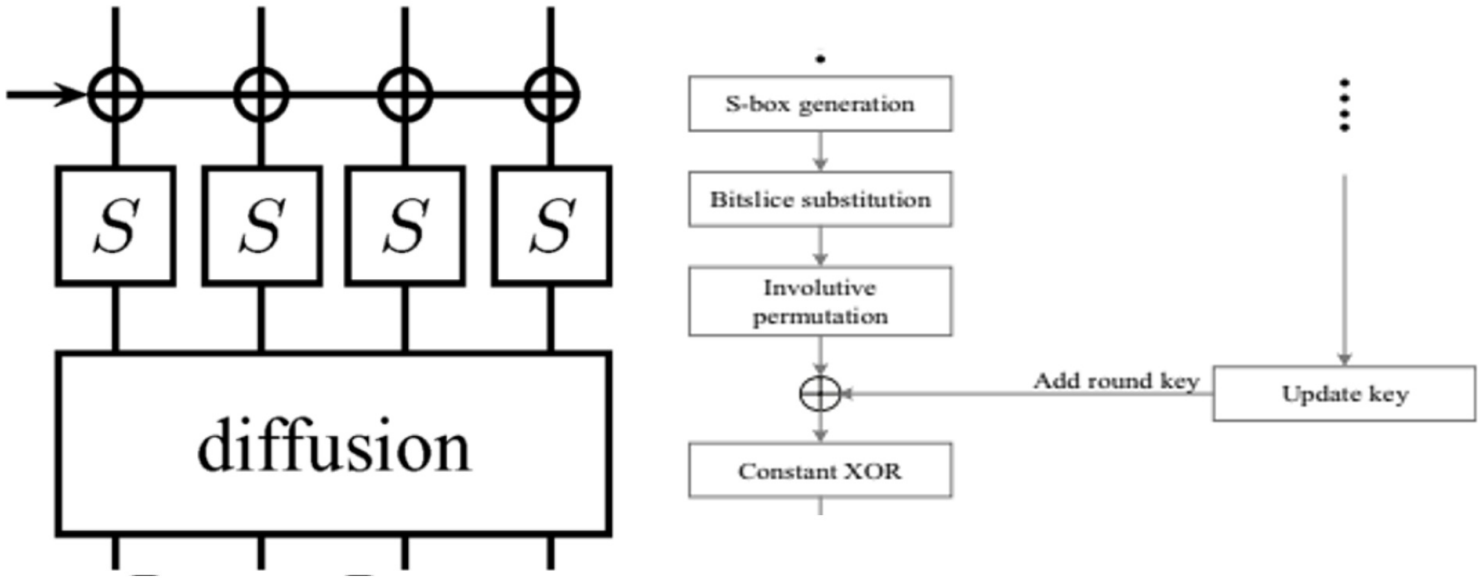


Figura: Comparación de round functions, Substitution-permutation network genérica y GIFT [4].

GIFT

Se coloca cada bit del plaintext en un bloque.

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

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

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

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

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

GIFT

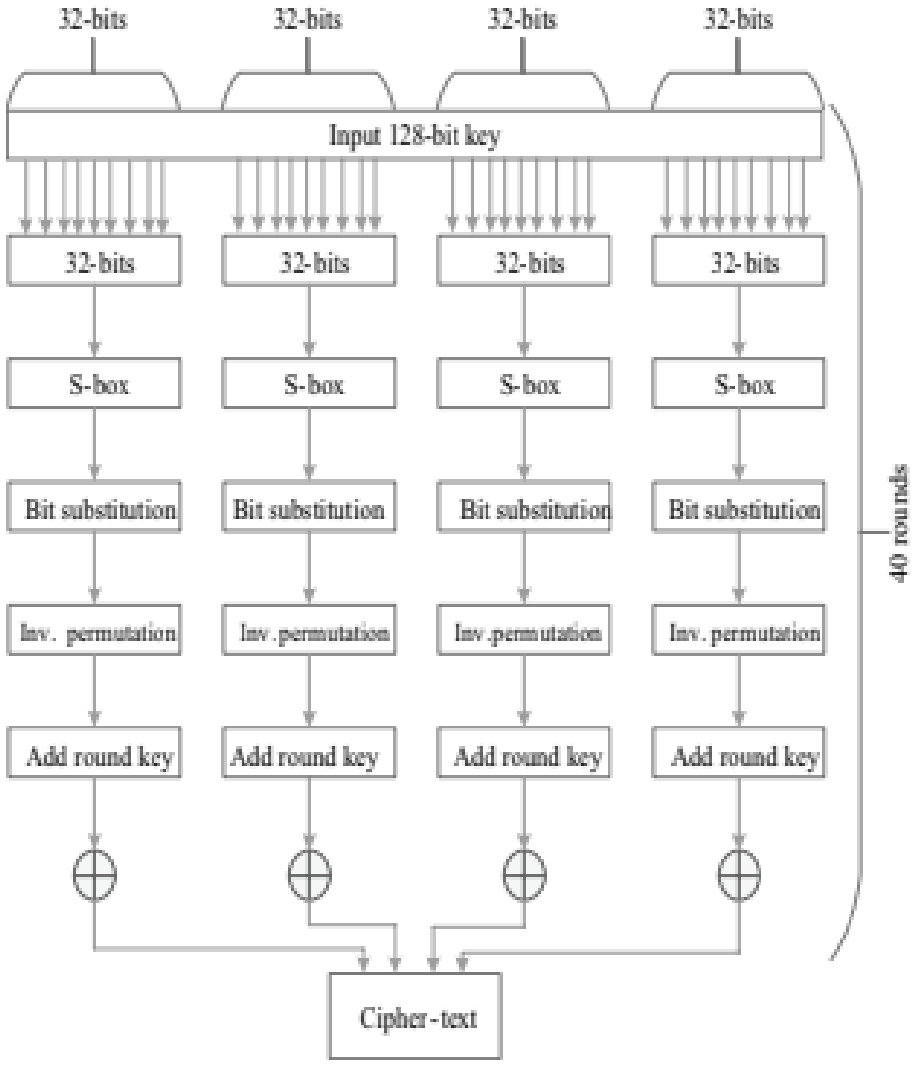


Figura: Representación secuencial de GIFT [4].

GIFT

La function bit-slice substitution es definida:

$$T_1 = X_1; T_2 = X_0 \wedge T_1; T_3 = X_2 \oplus X_3;$$
$$Y_0 = T_2 \oplus T_3; T_5 = X_3 \vee T_1; T_6 = X_0 \oplus T_5;$$
$$Y_1 = X_2 \wedge T_6; T_8 = X_1 \oplus X_2; T_9 = T_3 \wedge T_6;$$
$$Y_3 = T_8 \wedge T_9; T_{11} = Y_0 \vee T_8; Y_2 = T_6 \wedge T_{11}.$$

donde T_i indica una variable de 32-bits temporable. El bloque input es X y el bloque output es Y [4].

Conclusiones

Conclusiones

Feistel Network

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

Substitution-Permutation Network

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

References I

Y. Zhong and J. Gu, "Lightweight block ciphers for resource-constrained environments: A comprehensive survey," *Future Generation Computer Systems*, 2024.

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.

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 II

N. Yasmin and R. Gupta, "Modified lightweight gift cipher for security enhancement in resource-constrained iot devices," *International Journal of Information Technology*, pp. 1–13, 2023.

X. Huang, L. Li, and J. Yang, "Ivlbc: An involutive lightweight block cipher for internet of things," *IEEE Systems Journal*, 2022.

R. A. Ramadan, B. W. Aboshosha, K. Yadav, I. M. Alseadoon, M. J. Kashout, and M. Elhoseny, "Lbc-iot: Lightweight block cipher for iot constraint devices." *Computers, Materials & Continua*, vol. 67, no. 3, 2021.

S. Chen, Y. Fan, L. Sun, Y. Fu, H. Zhou, Y. Li, M. Wang, W. Wang, and C. Guo, "Sand: An and-rx feistel lightweight block cipher supporting s-box-based security evaluations," *Designs, Codes and Cryptography*, pp. 1–44, 2022.

References III

- D. Zhu, X. Tong, Z. Wang, and M. Zhang, "A novel lightweight block encryption algorithm based on combined chaotic system," *Journal of Information Security and Applications*, vol. 69, p. 103289, 2022.
- J. Feng and L. Li, "Scenery: a lightweight block cipher based on feistel structure," *Frontiers of Computer Science*, vol. 16, no. 3, p. 163813, 2022.
- V. Nachef, 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 cryptology*, vol. 9, no. 1, pp. 1–19, 1996.