Comparison Between Implemented Algorithms

Technology Library: UMC130

Operating Frequency: 100 MHz

	SIMON	RECTANGLE	HIGHT
Plaintext/Key size	32 / 64	64 / 80	64 / 128
Power (mW)	0.7596	1.485	1.783
Area (μm^2)	17,424	22,500	23,400
Throughput (Mbps)	92.5	246	200

It is noted that SIMON has the lowest power and area in the expense of security and throughput. However, HIGHT has higher security than RECTANGLE in expense of slight increase in power and area. RECTANGLE has the largest throughput through the three algorithms.

SIMON Compared to Literature

	SIMON	[1]	[2]
Technology	UMC130	ARM-130n	130n
Frequency	100 MHz	100 kHz	100 kHz
Plaintext/Key size	32 / 64	32 / 64	128 / 128
Power (μW)	759.6	-	1.32
Area (GE)	3,403	722	1,317
Throughput	92.5 Mbps	88.9 Kbps	22.9 Kbps

The implemented design has larger area than the one introduced in SIMON proposal [1] due to implementing decryption and controller modules. In addition, ARM library used in [1] has more flexibility than UMC130. Compared to [2], it is noted that the implemented design exhibits lower power consumption assuming $power\ \alpha\ f$. Also, it is noted that the throughput of the implemented design is much higher than the design in [2] as it is a bit serialized design.

RECTANGLE Compared to Literature

	RECTANGLE	[3]
Technology	UMC130	UMC130
Frequency	100 MHz	10 MHz
Plaintext/Key size	64 / 80	64 / 80
Power (μW)	1485	74.31
Area (GE)	4,395	1600
Throughput	246 Mbps	24.6 Mbps

The results obtained from [3] is only for encryption hardware, while our results are for both encryption and decryption hardware.

HIGHT Compared to Literature

	HIGHT	**[4]**	**[5]**	**[2]**
Technology	UMC130	250n	-	250n
Frequency	100 MHz	-	-	100 KHz
Power ($\boldsymbol{\mu W}$)	1783	-	1.32	5.48
Area ($\boldsymbol{GE}$)	4,570	722	1,317	3901
Throughput	200 Mbps	-	-	188.2 Kbps

The design in [4] is encryption only. Compared to [2], the implemented design will be better in terms of power.

References:

[1] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The simon and speck families of lightweight block ciphers," Cryptology ePrint Archive, Report 2013/404, 2013, http://eprint.iacr.orgI2013/404.

[2] I. Bhardwaj, A. Kumar, and M. Bansal, “A review on lightweight cryptography algorithms for data security and authentication in IoTs,” 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), 2017.

[3] W. Zhang et al., “RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms,” in Science China Information Sciences, 2015, vol. 58(12), pp. 1-15

[4] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, “HIGHT: A New Block Cipher Suitable for Low-Resource Device,” Lecture Notes in Computer Science Cryptographic Hardware and Embedded Systems - CHES 2006, pp. 46–59, 2006.

[5] P. Kitsos, N. Sklavos, M. Parousi, and A. N. Skodras, “A comparative study of hardware architectures for lightweight block ciphers,” Computers & Electrical Engineering, vol. 38, no. 1, pp. 148–160, 2012.