























- [1] A. K. Panda and K. C. Ray, "Design and FPGA Prototype of 1024-bit Blum-Blum-Shub PRBG Architecture," 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), Singapore, 2018, pp. 38-43, doi: 10.1109/ICICSP.2018.8549715.
- [2] Hassanzadeh, Alireza and Vahid Mahboubi. "A BBS Random Number Generator for Low Power Applications." *International Journal of Computer Applications* 131 (2015): 33-36.
- [3] C. Ding, "Blum-Blum-Shub generator," in *Electronics Letters*, vol. 33, no. 8, pp. 677-, 10 April 1997, doi: 10.1049/el:19970440.
- [4] K. Sewak, P. Rajput and A. K. Panda, "FPGA implementation of 16 bit BBS and LFSR PN sequence generator: A comparative study," 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, 2012, pp. 1-3, doi: 10.1109/SCEECS.2012.6184758.
- [5] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21.2 (1978): 120-126.
- [6] Cao, Zhengjun, Ruizhong Wei and Xiaodong Lin. "A Fast Modular Reduction Method." *IACR Cryptol. ePrint Arch.* 2014 (2014): 40.
- [7] Nozaki, Hanae, et al. "Implementation of RSA algorithm based on RNS Montgomery multiplication." *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, Berlin, Heidelberg, 2001.
- [8] Will, Mark A., and Ryan KL Ko. "Computing mod without mod." (2014).
- [9] Amandeep Singh, Praveen Agarwal, Mehar Chand. "Analysis and Development of Dynamic S-box Generation" *Computer Science and Information Technology* 2017
- [10] Tim Good and Mohammad Benaissia "AES on FPGA from fastest to smallest" *Department of Electrical and Electronic Engineering, University of Sheffield*
- [11] Manjith Baby Chellam and Ramasubramanian Natarajan "AES Hardware Accelerator on FPGA with Improved Throughput and Resource Efficiency" *Arabian Journal for Science and Engineering*
- [12] "Design and FPGA Implementation of UART Using Microprogrammed Controller" *Mohammad Awedh, Ahmed Mueen, Scholars Journal of Engineering and Technology*