iii	456	425	1	0	0	1	3	3
	125	81	0	1	1	-3	1	1
	81	44	1	-3	-1	4	1	1
	44	37	-1	4	2	-7	1	1
	37	7	2	-7	-3	11	9	1
iv	34	10	1	0	0	1	3	3
	10	4	0	1	1	-3	2	11

Finally, we get x = 2,527 and y = 183, therefore, $v = GCD\,(x, y) = GCD\,(2{,}527, 183)$ which can be calculated easily using Euclidian's algorithm.

3 LEAST COMMON MULTIPLE (LCM)

LCM is well known elementary number theory algorithm that is defined as the smallest multiple integer of two numbers. The very basic method to calculate LCM is using prime factorization method (PF-LCM).

PF-LCM method depends on fact that each integer number can uniquely written as a product of prime numbers raised to different powers. Then, we can calculate LCM by taking all common factors with greatest power.

An example of the algorithm is shown below:

40 = 235, 26 = 2.13➔ LCM (40, 26) = 23.5.13 = 520

Alternatively, LCM can be efficiently calculated by using the GCD reduction method [9]. LCM is usually calculated using GCD from the formula:

$$LCM\,(a,b) = \frac{ab}{\mathrm{GCD}\;(a,b)} = \left(\frac{a}{\mathrm{GCD}(a,b)}\right) b$$

Where GCD can be calculated using different algorithms without need to factor the numbers.

4 CONCLUSIONS

GCD/LCM operations are essential number theory algorithms that commonly used as underlying operations of many computing processors. The efficient utilization of such algorithms contributes in the overall leverage of system execution. For instance, Lehmer's algorithm reduces the large integers to common base (b) with fast convergence rate at complexity of O (n/log (n)) which make it faster than other algorithms. Eventually, Lehmer's algorithm can be efficiently implemented (in hardware or software) to compute both GCD and LCM operations for any two large integer numbers.

REFERENCES

[1]. A.J. Menezes, P.C. Van Oorschot and S.A. Vanstone. (1996). Handbook of Applied Cryptography", CRC Press, Boca Raton, Florida

[2]. W. Trappe and L. C. Washington, (2002) 'Introduction to Cryptography with Coding Theory', Prentice Hall, vol. 1: p.p. 1-176.

[3]. Q. Abu Al-Haija, M. Smadi, M. Jaffri and A. Shua'ibi, "Efficient FPGA Implementation of RSA Coprocessor Using Scalable Modules", 9th International Conference on Future Networks and Communications (FNC-2014), by Elsevier, Ontario, Canada, 17-20, Aug-2014.

[4]. M. R. K. Ariffin, M. A. Asbullah, N. A. Abu and Z. Mahad, " A New Efficient Asymmetric Cryptosystem Based on the Integer Factorization Problem of $\boldsymbol{N = p^2q}$", Malaysian Journal of Mathematical Sciences 7(S): 19-37 (2013)

[5]. K. J. Goldman, "Recursive Algorithms", Computer Science I, lecture notes, Washington University in St. Louis, 1997.

[6]. Q. A. Al-Haija, M. Al-Ja'fari and M. Smadi, (2016) 'A comparative study up to 1024-bit Euclid's GCD algorithm FPGA implementation & synthesizing', 2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), Ras Al Khaimah, United Arab Emirates, pp. 1-4.

[7]. D. Stehlé and P. Zimmermann (2004), "A binary recursive gcd algorithm", Algorithmic number theory (PDF), Lecture Notes in Comput. Sci., 3076, Springer, Berlin, pp. 411–425, MR 2138011, doi:10.1007/978-3-540-24847-7_31.

[8]. S. M. Sedjelmac, " On a Parallel Lehmer-Euclid GCD Algorithm", International Symposium on Symbolic and Algebraic Computation (ISSAC 2001), By ACM, UWO, Canada, 2001.

[9]. W. Stein, (2011) 'Elementary Number Theory: Primes, Congruence, and Secrets', Springer, vol. 1.

[10]. J. Sorenson. (1995). "An analysis of Lehmer's Euclidean GCD algorithm", Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation, pp. 254-258. Montreal, Canada, ACM Press.

[11]. Sidi Mohammed Sedjelmaci, "On a parallel Lehmer-Euclid GCD algorithm", Proceedings of the 2001 international symposium on Symbolic and algebraic computation, p.303-308, July 2001, London, Ontario, Canada. doi:10.1145/384101.384142
[12]. T. Jebelean. "A double-digit Lehmer–Euclid algorithm for finding the GCD of long integers", Journal of Symbolic Computation, 19 (1995), pp. 145-157
[13]. Jebelean, T., 1993. "A generalization of the binary GCD algorithm". In Proceedings of the 1993 international symposium on Symbolic and algebraic computation (pp. 111-116). ACM.
[14]. Wang, P.S., 1980. "The eez-gcd algorithm". ACM SIGSAM Bulletin, 14(2), pp.50-60.
[15]. Sasaki, T. and Suzuki, M., 1992. "Three new algorithms for multivariate polynomial GCD". Journal of symbolic computation, 13(4), pp.395-411.
[16]. T. Jebelean, "Comparing Several GCD Algorithms", ARITH-11: IEEE Symposium on Computer Arithmetic, 1993-June.
[17]. S. M. Sedjelmaci, "On a parallel extended Euclidean algorithm," Proceedings ACS/IEEE International Conference on Computer Systems and Applications, Beirut, 2001, pp. 235-241.