Table 5: Power Consumption of PaRSA-4 on Intel Core i3.

Process Technology: 90 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**$P_{LST\ PG}$**
1600	302.22	48.6	10.99	0.9	10.09	5.01
2100	302.22	63.73	10.99	0.9	10.09	5.01
2700	302.22	81.76	10.99	0.9	10.09	5.01
3300	302.22	99.79	10.99	0.9	10.09	5.01
Process Technology: 65 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**$P_{LST\ PG}$**
1600	163.03	26.67	14.84	1.4	13.44	6.71
2100	163.03	34.85	14.84	1.4	13.44	6.71
2700	163.03	44.66	14.84	1.4	13.44	6.71
3300	163.03	54.47	14.84	1.4	13.44	6.71
Process Technology: 45 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**$P_{LST\ PG}$**
1600	81.24	14.29	12.38	0.7	11.68	5.86
2100	81.24	18.63	12.38	0.7	11.68	5.86
2700	81.24	23.83	12.38	0.7	11.68	5.86
3300	81.24	29.03	12.38	0.7	11.68	5.86
Process Technology: 32 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**$P_{LST\ PG}$**
1600	44.49	7.89	15.5	0.81	14.69	7.41
2100	44.49	10.25	15.5	0.81	14.69	7.41
2700	44.49	13.08	15.5	0.81	14.69	7.41
3300	44.49	15.92	15.5	0.81	14.69	7.41
Process Technology: 22 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**$P_{LST\ PG}$**
1600	23.11	4.23	7.08	0.01	7.07	3.59
2100	23.11	5.47	7.08	0.01	7.07	3.59
2700	23.11	6.96	7.08	0.01	7.07	3.59
3300	23.11	8.44	7.08	0.01	7.07	3.59

Based on Table 6, it can be concluded that the most power-efficient Intel Core i5 configuration for PaRSA-4 is the configuration that is implemented at 22 nm feature size and runs at 1200 MHz i.e. Intel Core i5 (22 nm, 1200 MHz).Moreover, power gating techniques should be used to minimize leakage power contributions. In other words, the most power-efficient quad-core processor for the RSA should be implemented using small feature size and run at low clock frequency.

Table 6: Power consumption of PaRSA-4 on Intel Core i5.

Process Technology: 90 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**P_{LST_PG}**
1200	460.754	35.57	18.3	1.69	16.61	8.08
1500	460.754	44.31	18.3	1.69	16.61	8.08
1800	460.754	53.05	18.3	1.69	16.61	8.08
2100	460.754	61.79	18.3	1.69	16.61	8.08
2400	460.754	70.53	18.3	1.69	16.61	8.08
Process Technology: 65 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**P_{LST_PG}**
1200	253.17	20.04	26.1	2.59	23.51	11.51
1500	253.17	24.93	26.1	2.59	23.51	11.51
1800	253.17	29.81	26.1	2.59	23.51	11.51
2100	253.17	34.7	26.1	2.59	23.51	11.51
2400	253.17	39.58	26.1	2.59	23.51	11.51
Process Technology: 45 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**P_{LST_PG}**
1200	126.143	10.68	21.57	1.3	20.27	9.96
1500	126.143	13.25	21.57	1.3	20.27	9.96
1800	126.143	15.81	21.57	1.3	20.27	9.96
2100	126.143	18.38	21.57	1.3	20.27	9.96
2400	126.143	20.94	21.57	1.3	20.27	9.96
Process Technology: 32 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**P_{LST_PG}**
1200	70.38	5.87	26.77	1.48	25.29	12.5
1500	70.38	7.26	26.77	1.48	25.29	12.5
1800	70.38	8.64	26.77	1.48	25.29	12.5
2100	70.38	10.03	26.77	1.48	25.29	12.5
2400	70.38	11.41	26.77	1.48	25.29	12.5
Process Technology: 22 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**P_{LST_PG}**
1200	37.14	3.24	11.9	0.02	11.88	5.93
1500	37.14	3.98	11.9	0.02	11.88	5.93
1800	37.14	4.27	11.9	0.02	11.88	5.93
2100	37.14	5.46	11.9	0.02	11.88	5.93
2400	37.14	6.2	11.9	0.02	11.88	5.93

It should also be equipped with leakage-mitigation techniques as the processor becomes more leakage-consuming at low process technologies. By taking the Intel Core i5 (90 nm, 1200 MHz) as a base case, the power-efficient configuration can achieve around 82.6 % power saving. On the other hand,

considering the Intel Core i5 (90 nm, 2400 MHz) as a reference case, the power-efficient configuration can achieve approximately 89.6% power saving. On

the other hand, Table 7 illustrates the power consumption of PaRSA-8 on Intel Core i7. It also gives the total processor area under all feature sizes. By analyzing the power consumption values provided in Table 7, it becomes apparent that the same observations that have been made based on Table 4, 5 and 6 applies also to Intel Core i7.

Table 7: Power consumption of PaRSA-8 on Intel Core i7.

Process Technology: 90 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**P_{LST_PG}**
1200	506.012	38.15	19.03	1.78	17.25	8.38
1500	506.012	47.53	19.03	1.78	17.25	8.38
1800	506.012	56.91	19.03	1.78	17.25	8.38
2100	506.012	66.3	19.03	1.78	17.25	8.38
2400	506.012	75.68	19.03	1.78	17.25	8.38
Process Technology: 65 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**P_{LST_PG}**
1200	278.038	21.16	27.31	2.74	24.57	12.01
1500	278.038	26.32	27.31	2.74	24.57	12.01
1800	278.038	31.48	27.31	2.74	24.57	12.01
2100	278.038	36.65	27.31	2.74	24.57	12.01
2400	278.038	41.81	27.31	2.74	24.57	12.01
Process Technology: 45 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**P_{LST_PG}**
1200	138.492	11.24	22.61	1.38	21.23	10.42
1500	138.492	13.49	22.61	1.38	21.23	10.42
1800	138.492	16.65	22.61	1.38	21.23	10.42
2100	138.492	19.35	22.61	1.38	21.23	10.42
2400	138.492	22.65	22.61	1.38	21.23	10.42
Process Technology: 32 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**P_{LST_PG}**
1200	76.93	6.17	28.11	1.59	26.54	13.1
1500	76.93	7.63	28.11	1.59	26.54	13.1
1800	76.93	9.09	28.11	1.59	26.54	13.1
2100	76.93	10.55	28.11	1.59	26.54	13.1
2400	76.93	12.01	28.11	1.59	26.54	13.1
Process Technology: 22 nm						
Frequency (MHz)	**Area (mm^2)**	**P_D(W)**	**P_L (W)**			
			Total	**P_{LG}**	**P_{LST}**	**P_{LST_PG}**
1200	40.48	3.4	12.51	0.02	12.49	6.22
1500	40.48	4.18	12.51	0.02	12.49	6.22
1800	40.48	4.96	12.51	0.02	12.49	6.22
2100	40.48	5.75	12.51	0.02	12.49	6.22
2400	40.48	6.63	12.51	0.02	12.49	6.22

It can be observed that PaRSA-8 consumes its lowest power on Intel Core i7 (22 nm, 1200 MHz) with power gating capability. In other words, the most power-efficient processor for PaRSA-8 is an octa-core processor implemented using small feature size and is operated at low clock rate. By taking Intel Core i7 (90 nm, 1200 MHz) as a reference case, Intel Core i7 (22 nm, 1200 MHz) achieves around 83.1% power saving. On the other hand, by taking Intel Core i7 (90 nm, 2400 MHz) as our reference case, the power-efficient configuration can achieve around 89.8% power saving.

5.3 Energy Dissipation Analysis

This section shows the energy that PaRSA-*n* consumes on the processor configurations shown in Table 1. For each configuration, *n* is set to the number of hardware threads supported by that configuration; this is the situation where PaRSA-*n* achieves its optimal performance. The total energy that PaRSA-*n* dissipates on a particular processor depends on its execution time and the total power consumed by the processor. In other words:

$$Energy = Power * Execution\ Time \quad (9)$$

Fig.11 depicts the total energy consumed by PaRSA-2 on Intel Core2Duo processor. It shows the total energy under all possible clock frequencies and feature sizes. The total energy is the sum of dynamic and leakage energies. In Fig.11, the x-axis of each subplot indicates the process technology while the y-axis shows the total energy. Each subplot corresponds to a particular clock frequency. It can be observed that, at all clock frequencies, PaRSA-2 has consumed its lowest energy when the processor was implemented using the 22 nm process technology. In addition, the most energy-efficient configuration is the Intel Core2Duo (22nm, 2800 MHz). Although the Intel Core2Duo (22 nm, 800MHz) was the Most power-efficient configuration (section 5.2), it consumes more energy that Intel Core2Duo (22 nm, 2800 MHz). This is due to the fact that processor energy depends not only on its power consumption but also on its execution time. The execution time of PaRSA-2 on Intel Core2Duo (22nm, 2800MHz) is less than its execution time on Intel Core2Duo (22nm, 800MHz); the magnitude of execution time reduction is higher than power consumption increases as PaRSA-2 moves from Intel Core2Duo (22 nm, 800MHz) to Intel Core2Duo (22 nm, 2800 MHz). Whereas Intel Core2Duo (22 nm, 2800 MHz) has a 71.70% reduction in execution time as compared to Intel Core2Duo (22 nm, 800 MHz), it has a 58.03% increases in its total power consumption. Therefore, its execution time reduction offsets its power consumption increase which in turn leads to less energy dissipation as compared to Intel Core2Duo (22 nm, 800 MHz).

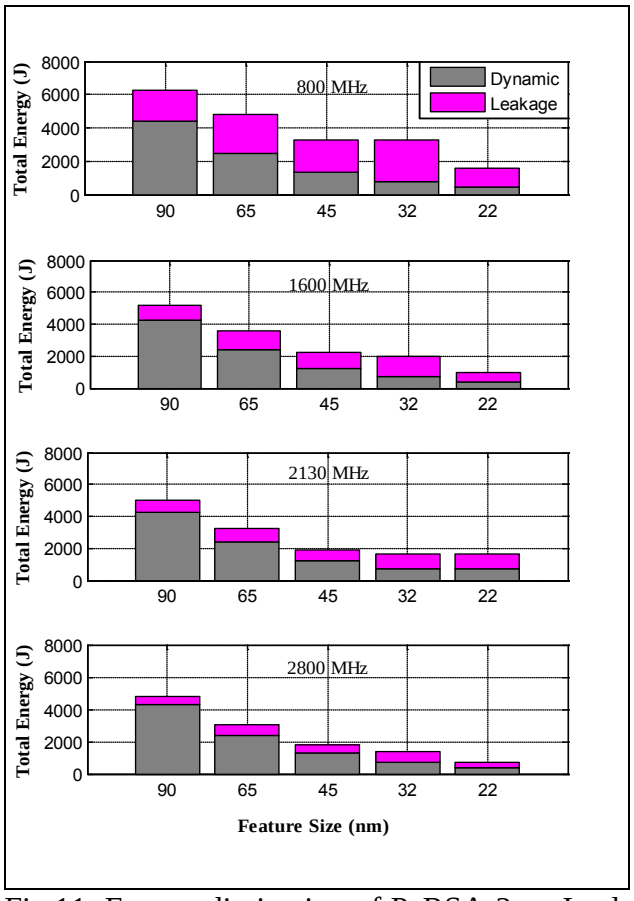

Fig.11: Energy dissipation of PaRSA-2 on Intel Core2Duo.

On the other hand, Fig.12 illustrates the energy dissipation of PaRSA-4 on Intel Core i3 processor. it shows the total energy dissipated at all possible clock rates and process technologies. Based on Fig.12, it can be observed that the most energy-efficient Intel core i3 configuration for PaRSA-4 is the Intel Core i3 (22 nm, 3300 MHz). compared with the results shown in Table 5, the most energy-efficient configuration for PaRSA-4 is not necessarily equivalent to the most power efficient configuration since the total processor energy is a

function both power consumption and execution time.

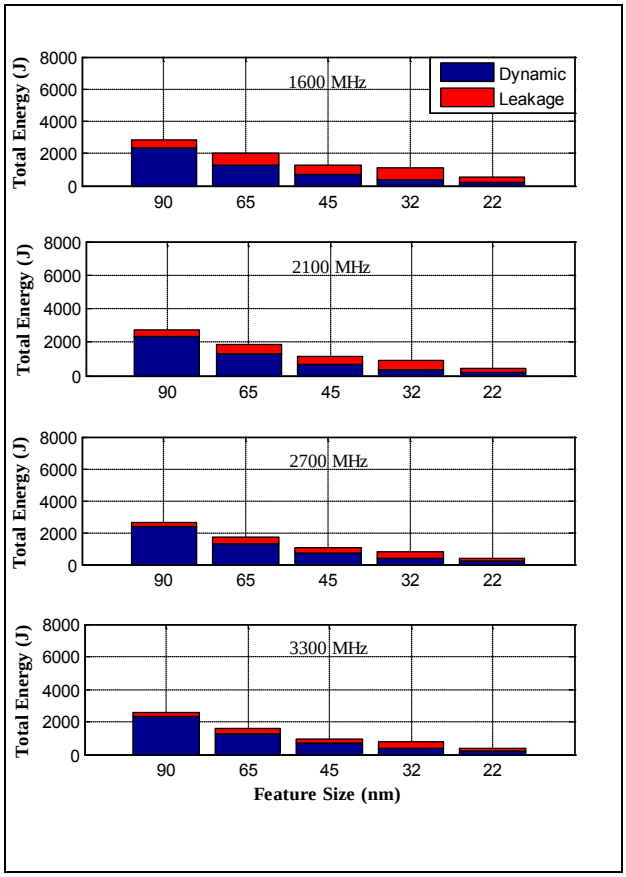

Fig.12: Energy Dissipation of PaRSA-4 on Intel Core i3.

Intel Core i3 (22 nm, 3300) has a 37.2% increase in its power consumption as compared to the Intel Core i3 (22 nm, 1600 MHz) i.e. the most power-efficient configuration. Moreover, it has achieved a 51.3% reduction in the execution time of PaRSA-4 as compared to the Intel Core i3 (22 nm, 1600 MHz). Therefore, the percent reduction in execution time outweighs the percent increase in the total power consumption which has led to an overall reduction in the total energy dissipation of the Intel Core i3 (22 nm, 3300 MHz) as it executes PaRSA-4. Fig.13 shows the total energy dissipation of PaRSA-4 on Intel Core i5 processor. The energy values are shown for each possible pair of process technology and clock rate supported by this processor. The results given by Fig.13 indicate that the most energy-efficient Intel Core i5 configuration for PaRSA-4 is that implemented at 22 nm and run at 2400 MHz i.e. Intel Core i5 (22 nm, 2400 MHz).Similar to the previous processor configurations, the energy-efficient configuration of Intel Core i5 is different from the power-efficient configuration which was found to be Intel Core i5 (22 nm, 1200 MHz). Compared to the Intel Core i5 (22 nm, 1200 MHz), Intel Core i5 (22 nm, 2400 MHz) has a 19.6% increase in power consumption and 50.8% reduction in execution time.

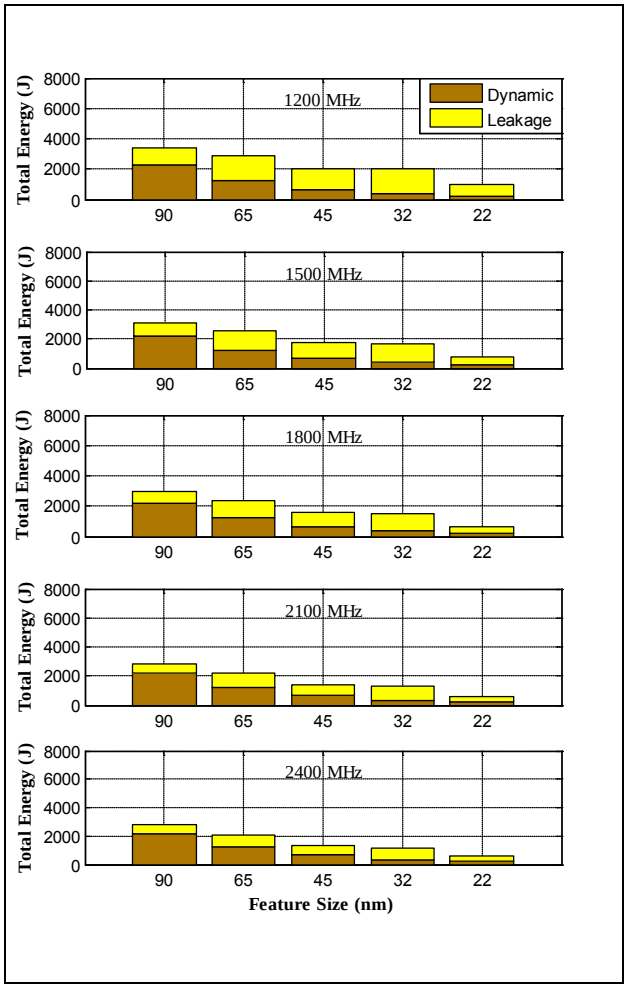

Fig.13: Energy Dissipation of PaRSA-5 on Intel Core i5.

Therefore, an overall energy saving has been achieved. So far, there are two energy-efficient processor configurations for PaRSA-4: Intel Core i3 (22nm, 3300 MHz) and Intel Core i5 (22 nm, 2400 MHz). our results indicate that PaRSA-4 has a 593.091 Joules of energy dissipation and a 31.11 seconds of execution time on Intel Core i5 (22 nm, 2400 MHz). on the other hand, it has a 363.478 Joules of energy and a 23.42 seconds of execution time on Intel Core i3 (22 nm, 3300 MHz). In other words, Intel Core i3(22 nm , 3300 MHz) has achieved a 35.5% reduction in energy and a 24.7% reduction in execution time as compared to the Intel Core i5 (22 nm, 2400 MHz). Although the two processors support the same number of hardware thread, Intel Core i3 has outperformed Intel Core i5

due to its high clock frequency; it has a lower execution time and lower energy dissipation. In summary, it can be concluded that the best Multicore processor configuration, in terms of performance and energy, for PaRSA-4 is a processor that supports four simultaneous hardware threads and runs at a high clock rate. However, this observation should be further investigated based on the lifetime reliability of the processor as will be shown in the next subsection.

Fig.14 illustrates the energy dissipation of PaRSA-8 on Intel Core i7. The total energy dissipation has been shown for all possible combinations of process technology and clock rate.

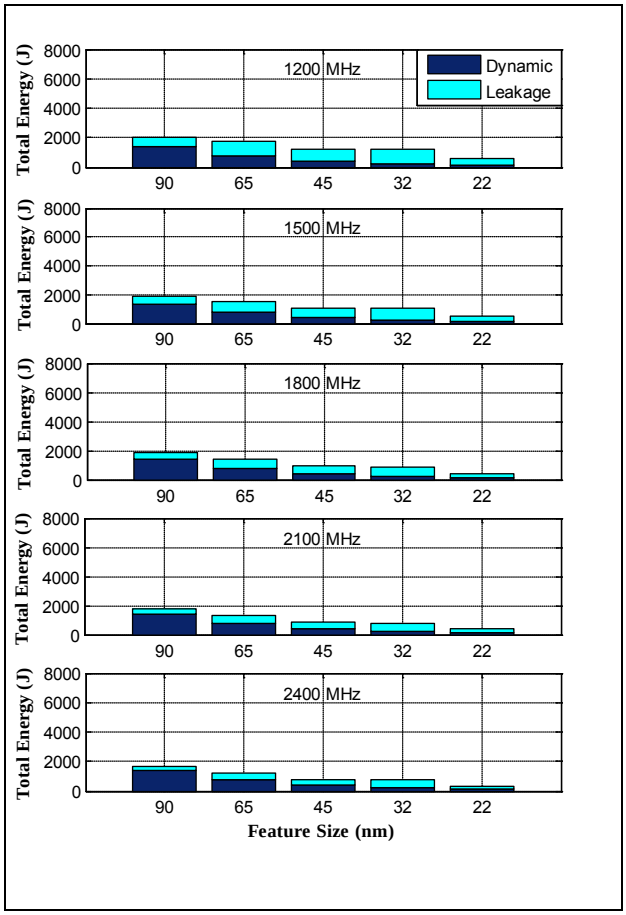

Fig.14: Energy Dissipation of PaRSA-8 on Intel Core i7.

Fig.14 implies the fact that the most energy-efficient process technology and clock rate, of Intel core i7, are 22 nm and 2400 MHz respectively. This observation confirms the aforementioned fact that the power-efficient configuration and the energy-efficient configuration are not necessarily equivalent. Whereas the power-efficient configuration for PaRSA-8 was the Intel Core i7 (22 nm, 1200 MHz), the energy-efficient configuration is the Intel Core i7 (22 nm, 2400 MHz). The energy-efficient configuration has a 19.7% increase in power consumption and 49.9% reduction in execution time as compared to the power-efficient configuration. Thus, an overall energy saving has been achieved since the amount of execution time reduction is greater than the amount of power increase. Therefore, it can be observed that the best Multicore processor configuration for PaRSA-8 from energy perspective is a processor that supports 8 hardware threads and runs at a high clock rate. Based on the results shown in this section, the most energy-efficient configurations for PaRSA-2, PaRSA-4 and PaRSA-8 are Intel Core2Duo (22 nm, 2800 MHz), Intel Core i3 (22 nm, 3300 MHz) and Intel Core i7 (22 nm, 2400 MHz) respectively.Table 8 summarizes the execution time and the total energy of the optimal configurations for PaRSA-*n* where *n* is the number of hardware threads supported by the associated processor. The term optimal refers to the processor configuration that has achieved the lowest execution time and energy dissipation among all configurations that support the same number of hardware threads.

Table 8: PaRSA-n Optimal Configuration Parameters.

Algorithm	**Configuration**	**Energy (Joules)**	**Time (Seconds)**
PaRSA-2	Intel Core2Duo (22 nm, 2800 MHz)	700.994	45.08
PaRSA-4	Intel Core i3 (22 nm, 3300 MHz)	363.4784	23.42
PaRSA-8	Intel Core i7 (22 nm, 2400 MHz)	341.5776	17.94

The observation that can be made based on Table 8 is that PaRSA-*n* can achieve a substantial performance improvement and energy savings by increasing the number of hardware threads and using a processor configuration whose number of hardware threads is at least equal to *n*. PaRSA-8 has achieved a 60.2 % performance improvement as compared to PaRSA-2 and a 23.4 % performance

improvement as compared to PaRSA-4. On the other hand, it has achieved a 51.3 energy saving as compared to PaRSA-2 and a 6.03 % energy saving as compared to PaRSA-4. Therefore, from performance and energy perspectives, PaRSA-8 is the best implementation of the RSA algorithm and Intel Core i7 (22 nm, 2400 MHz) is the optimal processor configuration for this algorithm. However, this result should be further investigated in terms of lifetime reliability as will be shown in the next subsection.

5.4 Lifetime Reliability Analysis

This section shows the lifetime reliability of the different processor configurations under the PaRSA-*n* workload. In section 5.3, it has been shown that all the energy-efficient configurations were obtained at the same process technology. Consequently, only clock rate has been considered for the sake of reliability analysis. As shown in section 4.3, the reliability analysis framework relies mainly on processor temperature in order to quantify its lifetime reliability [40-42]. Hence, it is necessary to obtain the temperature of the processor at different clock rates. In order to achieve this goal, the psensor [48] utility has been used to read the temperature of the processor while a particular PaRSA-*n* workload is running. In order to estimate the lifetime reliability at clock rates other than those supported by the real hardware, an empirical model has been developed. This model captures the relationship between processor's temperature and its clock rate and can be used to predict processor's temperature at each possible clock rate. Fig.15 illustrates the relationship between processor temperature and its clock rate. The temperatures obtained by psensor were first plotted and a curve-fitting operation has been performed to obtain a mathematical formula that expresses processor temperature as a function of its clock rate. It can be observed that there is a quadratic relationship between processor temperature and its clock rate. The temperature values obtained by the psensor utility or the developed model have then be input to the RAMP model [40-42] in order to get an estimate of the processor's lifetime reliability as it runs a particular PaRSA-*n* workload. Fig.16 depicts the mean time to failure (MTTF) as a function of clock frequency. It shows the MTTF based on each of the physical failure mechanisms described in section 4.3. The x-axis indicates the clock rate, while the y-axis shows the MTTF as a function of the clock rate. Each subplot is labeled with the corresponding failure mechanism.

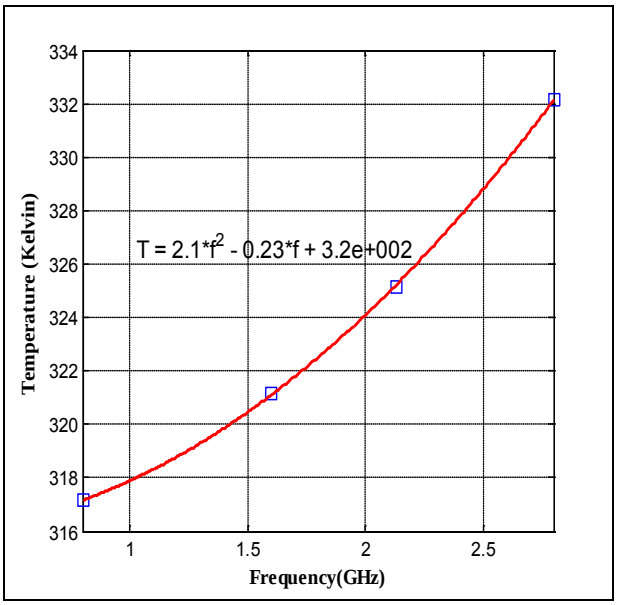

Fig.15: The Relationship between processor temperature and its clock rate.

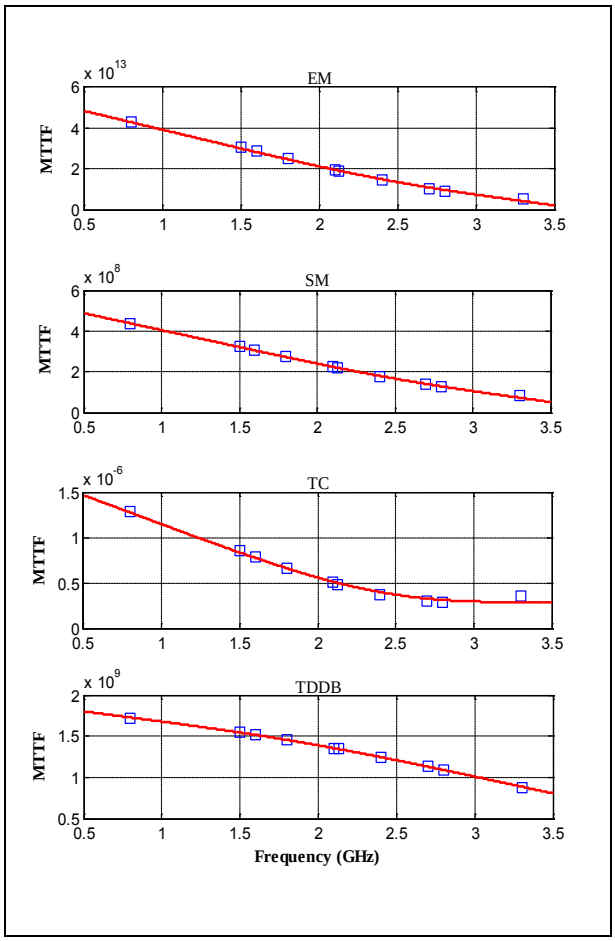

Fig.16: Processor's MTTF as a function of clock rate.

Fig.16 illustrates the fact that the MTTF of a processor is a decreasing function of clock rate. In other words, a processor running at a low clock rate would sustain a longer period of time before encountering temperature-induced failures as compared to a processor that runs on a higher clock rate. Therefore, it is important to re-evaluate the optimal configurations specified in section 5.3 based on the lifetime reliability of the processor. Table 9 shows a comparison between the power-efficient and the energy-efficient configuration for each PaRSA-*n*. It shows the percent increase in MTTF that the power- efficient configuration can achieve as compared to the energy-efficient configuration for each PaRSA-*n* under all possible physical failure mechanisms. The comparison results have been reported in terms of the percent increase in MTTF values since processor reliability is directly proportional to its MTTF.

Table 9: MTTF comparison.

Algorithm	MTTF (EM)	MTTF (SM)	MTTF (TDDB)	MTTF (TC)
PaRSA-2	368.5%	251.2%	59.26%	333.3%
PaRSA-4	458.82%	280.25%	72.73%	100.1
PaRSA-8	146.58%	112.43%	30.40%	150%

As shown in sections 5.2 and 5.3, power-efficient configurations have lower clock rates than the energy-efficient ones. Therefore, they exhibit low heat dissipation and spans a longer lifetime as compared to energy-efficient processors that run at higher clock rates. This fact can be directly observed from Table 9 which shows that moving from energy-efficient configuration (i.e. higher clock rate) to power-efficient configuration (i.e. lower clock rate) results into a significant increase in processor reliability under various physical failure mechanisms. Taking lifetime reliability into consideration, the optimal configurations for PaRSA-2, PaRSA-4 and PaRSA-n will be Intel Core2Duo (22 nm, 800 MHz), Intel Core i3 (22 nm, 1600 MHz) and Intel Core i7 (22 nm, 2400 MHz) respectively. Based on the results shown in this section, it can be observed that the optimal processor configuration for RSA is a Multicore processor with a large number of hardware threads, low clock rate and a small feature size.

6. Conclusion

In this paper, an extensive design space exploration (DSE) has been performed in order to figure out the optimal Multicore processor configuration for cryptographic algorithms. All experiments were based on a parallel version of the RSA algorithm tuned for optimal performance settings. Our results indicate that a careful balance between processor specifications i.e. Clock rate, number of hardware threads and process technology should be achieved in order to obtain the optimal processor configuration that maintains a reasonable tradeoff between performance, power consumption, energy dissipation and lifetime reliability of the processor. However, the appropriate setting of processor specifications depends on the design constraints and system requirements.

References:

[1] www.us-cert.gov.

[2] J. Pieprzyk and David Pointcheval, *Parallel Authentication and Public key encryption. Information Security and Privacy*, Lecture notes in computer science, Vol. 2727, 2003,pp. 387-401.

[3] R. L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, Vol. 21, Issue 2, 1978, pp. 120-126.

[4] P Barrett, *Implementating the Rivest, Shamir and Aldham Public-key Encryption Algorithm on Standard Digital Signal Processor*, Proceedings of CRYPTO'86, Lecture Notes in Computer Science, 1986, pp. 311–323.

[5] B. Chapman, G. Jost, and R. V. D. Pas, *Using OpenMP: Portable Shared Memory Parallel Programming (Scientific and Engineering Computation)*, The MIT Press, 2007.

[6] A. J. Menezes, S. A. Vanstone and P. C. V. Oorschot, *Handbook of Applied Cryptography*, CRC Press, Inc., Boca Raton, FL, USA, 1986.

[7] C. Fu and Z.-L Zhu, An Efficient *Implementation of rsa Digital Signature*

Algorith,. In Proc. of the 4th International Conference on Wireless Communications, Networking and Mobile Com-puting, 2008, pp. 1–4.

[8] W. Diffie and M. Hellman, *New Directions in Cryptography*, IEEE Transactions on Information Theory, Vol. 22, No. 6, 1976, pp. 644–654.

[9] P. Hamalainen, N. Liu, M. Hannikainen and T. D. Hamalainen, *Acceleration of Modular Exponentiation on System-on-a-Programmable-Chip,* In. Proc. of the International Symposium of the system-on-Chip, 2005, pp. 14-17.

[10] K. Skadron, P. S. Ahuja, M. Martonosi and D. W. Clark, *Branch Prediction, Instruction-Window Size, and Cache Size: Performance Trade-Offs and Simulation Techniques*, IEEE Transactions on Computers, Vol. 48, Issue 11, 1999, pp. 1260-1281.

[11] A. Gellert, G. Palermo, V. Zaccaria, A. Florea, L. Vintan and C. Silvanto, *Energy-Performance Design Space Exploration in SMT Architectures Exploiting Load Value Predictions,* In Proc. of the Design Automation and Test in Europe Conference and Exhibition (Date), 2010, pp. 271-274.

[12] S. K. Dash, T. Srikanthan, *Instruction Cache Tuning for Embedded Multitasking Applications,* In Proc. of the IEEE/IFIP International Symposium on Rapid System Prototyping, 2009, pp. 152-158.

[13] T. S. R. Kumar, C. P. Ravikumar and R. Govindarajan, *Memory Architecture Exploration Framework for Cache Based Embedded SoC,* In Proc. of the 21st International Conference on VLSI Design, 2008, pp. 553-559.

[14] M. Y. Qadri and K. D. M. Maier, *Data Cache Energy and Throughput Models: Design Exploration for Embedded Processor,* EURASIP Journal on Embedded Systems, 2009 , Article 13 (Jan. 2009).

[15] A. G. Silva-Filho, F. R. Cordeiro, C. C. Araujo, A. Sarmento, M. Gomes, E. Barros and M. E. Lima, *An ESL Approach for Energy Consumption Analysis of Cache Memories in SoC Platforms,* International Journal of Reconfigurable Computing, Vol. 2011, pp. 1-12,2011.

[16] S. Przybylski, M. Horowitz and J. Hennessy, *Performance Tradeoffs in Cache Design,* In Proc. of the 15th Annual International Symposium on Computer Architecture, 1988, pp. 290-298.

[17] M. Alipour and M. E. Salehi, *Design Space Exploration to Find the Optimum Cache and Register File Size for Embedded Applications,* In Proc. of the 9th International Conference on Embedded Systems and Applications, 2011, pp. 214-219.

[18] M. Alipour, H. Taghdisi and S. H. Sadeghzadeh, *Multi objective design space exploration of cache for embedded applications,* In. Proc. of the 25th IEEE Canadian Conference on Electrical and Computer Engineering, 2012, pp.1-4.

[19] Y. Cai, M. T. Schmitz, A. Ejlali, B. Al-Hashimi and S. R. Reddy, *Cache Size Selection for Performance, Energy and Reliability of Time-Constrained Systems,* In Proc. of Asia and South Pacific Conference on Design Automation, 2006, pp. 923-928.

[20] M. Alipour and H. Taghdisi, *Effect of Thread Level Parallesim on the Performance of Optimum Architecture for Embedded Applications,* International Journal of Embedded systems and Applications. Vol. 2, No. 1, 2012, pp. 15-24.

[21] S. Eyerman, L. Eeckhout and K. D. Bosschere, *Efficient Design Space Exploration of High Performance Embedded Out-of-Order Processors,* In. Proc. of Design Automation and Test in Europe, 2006, pp. 1-6.

[22] G. Palermo, C Silvano and V. Zaccaria, *Multi-objective Design Space Exploration of Embedded Systems, Journal of Embedded Computing,* Vol. 1, Issue 3, 2005, pp. 305-316.

[23] A. Assaduzzamn, F. Sibai and M. Rani, *Impact of level-2 Cache Sharing on the Performance and Power Requirements of Homogenous Multicore Embedded Systems,* Microprocessors

and Microsystems, Vo. 33,Issue 5-6, 2009, pp. 388-397.

[24] A. Assaduzzamn and M. Rani, *Level-2 Shared Cache versus Level-2 Dedicated Cache for Homogenous Multicore Embedded Systems,* In Proc. of the 7th International Conference on Computing, Communications and Control Technologies, 2009.

[25] A. Assaduzzaman, M. Rani and F. Sibai, *On the Design of Low-Power Cache Memories for Homogenous Multicore Processor*, In Proc. of the 22nd International Conference on Microelectronics, 2010, pp. 387-390.

[26] A. Assaduzzaman, *A Power-Aware Multi-Level Cache Organization Effective for Multicore Embedded Systems,* Journal of Computers, Vol. 8, No. 1, 2013, pp. 49-60.

[27] F. Sibai, *On the Performance Benefits of Sharing and Privatizing Second and Third Level Cache Memories in Homogenous Multi-core Architectures,* Microprocessors and Microsystems, Vol. 32, Issue 7 , 2008, pp. 405-412.

[28] V. Saravanan, S. K. Chandran, S. Punnekkat and D. P. Kothari, *A Study on the Factors Influencing Power Consumption in Multithreaded and Multicore CPUs,* WSEAS Transactions on Computers, Vol. 10, Issue 3, 2011, pp. 93-103.

[29] W. Bielecki and D. Burak, *Parallelization of the AES Algorithm,* In. Proc. of the 4th WSEAS International Conference on Information Security, Communications and Computers,2005, pp.224-228.

[30] S. Saxena, N. Kishore, D. Handa and B. Kapoor, *Comparative Analysis of Sequential and Parallel Implementations of RSA,* International Journal of Scientific and Engineering Research, Vol. 4, Issue 8, 2013,pp. 2100-2103.

[31] V. Garg and V. Arunachalam, *Architectural Analysis of RSA Cryptosystem on FPGA,* International Journal of Computer Applications, Vol. 26, No. 8, 2011, pp. 30-34.

[32] M. Hill and M. Marty, *Amdahl's law in the Multicore era,* IEEE Computer, vol. 41, no. 7, 2008, pp.33 -38.

[33] S. Akther and J. Roberts, *MultiCore Programming: Increasing Performance through Software Multi-threading,* The Intel Press, 2006.

[34] www.fedoraproject.org.

[35] www.intel.com.

[36] wiki.archlinux.org.

[37] S. Li, J. H. Ahn, R. D. Strong, J. B. Brockman, D. M. Tullsen and N. P. Jouppi, *The McPAT Framework for Multicore and Manycore Architectures: Simultaneously Modeling Power, Area and Timing,* ACM Transactions on Architecture and Code Optimization.,Vol. 10, No. 1 , 2013, Article 5.

[38] www.itrs.net.

[39] R. Ubal, B. Jang, P. Mistry, D. schaa and D. Kaeli, *Multi2Sim: a simulation framework for CPU-GPU computing,* In Proc. of the 21st International Conference on Parallel Architectures and Compilation Techniques, 2012, pp. 335-344.

[40]J. Srinivasan, S. V. Adve, P. Bose and J. Rivers, *The Case for Lifetime Reliability-Aware Microprocessors,* In Proc. of the 31st International Symposium on Computer architecture, 2004, pp. 276-287.

[41] J. Srinivasan, S. V. Adve, P. Bose and J. Rivers, *Lifetime Reliability: Toward an Architectural Solution,* IEEE Micro, Vol. 25, Issue 3, 2005, pp. 70-80.

[42] J. Srinivasan, S. V. Adve, P. Bose and J. Rivers, *The Impact of Technology Scaling on Lifetime Reliability,* In Proc. of the International Conference on Dependable Systems and Networks, 2004, pp. 177-186.

[43] D. A. Patterson and J. L. Hennessy, *Computer Architecture: a Quantitative Approach*, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA,2006.

[44] J. J. Clement, *Electromigration Modeling for Integrated Circuit Interconnect Reliability Analysis*, IEEE Transactions on Device and Materials Reliability. Vol. 1, Issue 1, 2001, pp. 33-42.

[45] Yi- L. Cheng, B-J. Wei and Yi-L. Wang, *Scaling Effect on Electromigration in Copper Interconnects*, In Proc. of the 16th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits, 2009, pp. 698-701.

[46]J. H. Stathis, *Reliability limits for the gate Insulator in CMOS technology*, IBM Journal of Research and Development, Vol. 46, 2002, pp. 265-286.

[47] E. Wu, J.Sune, W. Lai, E. Nowak, J. McKenna, A. Vayshenker and D. Harmon, *Interplay of voltage and temperature acceleration of oxide breakdown for ultra-thin gate oxides. Solid-state Electronics Journal*, Vol. 46, 2002, pp. 1787-1798.

[48] https://aur.archlinux.org/packages/psensor.

[49] S. Borkar, *Design Challenges of Technology Scaling*, IEEE Micro, Vol. 19, Issue 4, 1999, pp. 23-29.

[50] A. P. Chandrakasan, S. Sheng and R. W. Brodersen, *Low-power CMOS Digital Desig, IEEE Journal of Solid-state Circuits*.Vol. 27, Issue 4, 1992, pp.473-484.