Preliminary Hardware Benchmarking of a Group of Round 2 NIST Lightweight AEAD Candidates

Mustafa Khairallah, Thomas Peyrin and Anupam Chattopadhyay

Nanyang Technological University, Singapore

Abstract. In this report, we analyze the hardware implementations of 10 candidates for Round 2 of the NIST lightweight cryptography standardization process. These candidates are Ascon, DryGASCON, Elephant, Gimli, PHOTON-Beetle, Pyjamask, Romulus, Subterranean, TinyJAMBU and Xoodyak. Specifically, we study the implementations of these algorithms when synthesized using the TSMC 65nm and FDSOI 28nm technologies and Synopsys Design Compiler, targeting various performance trade-offs and different use-cases. We show how different candidates stack-up against such trade-offs. We base our benchmarking parameters and metrics on real-world use-cases, such as high-speed applications, lightweight communication protocols and internet payloads.

Keywords: ASIC · authenticated encryption · AEAD · lightweight cryptography · NIST · benchmarking

1 Introduction

Lightweight Symmetric Key Cryptography has been a growing research area in the past 10 years or more, with applications varying from block cipher design to authenticated encryption or hash functions and much more. This has led the National Institute of Standards and Technology (NIST) to release a call for proposals to establish a new lightweight cryptography standard [NIS18]. The goal is to use the standardized primitive(s) in applications such as Internet-of-Things (IoT) and Sensor Networks. Authenticated Encryption with Associated Data (AEAD) is one of the most important requirements of symmetric key cryptography (SKE) in these environments, since it is usually cheaper than having independent solutions for the authentication and encryption requirements of the system. NIST received 57 submissions. 56 submissions were accepted into round 1 of the process, and after a rigorous period of analysis 32 designs were selected for round 2. Round 2 is expected to last till December, 2020. Hence, we have decided to study the ASIC performance of different Round 2 candidates.

Why ASIC? We have chosen to study ASIC implementations for two main reasons:

1. ASIC is an important technology in practice, since many real world products rely on ASIC accelerators for improving the performance of cryptographic algorithm. This is evident by the wide adoption of ASIC accelerators for the high performance implementations of Advanced Encryption Standard (AES) and standard hash functions such as SHA-2 and SHA-3. However, due to either expensive tools, lack of expertise, or simplicity of other technologies, *e.g.*, FPGA or micro-controllers, ASIC benchmarking and estimations are sometimes overlooked. During the CAESAR competition [CAE20], ASIC benchmarking was not thoroughly studied except at the late stages of the competition [KHYKC17]. Having early ASIC benchmarks will

help the designers improve the performance of their algorithms and give a better perspective about the comparative evaluation of the candidates.

2. Several benchmarking projects have been launched targeting micro-controllers [SR20], general-purpose processors [BL20] or FPGA [MHN+20]. However, in absence of an ASIC evaluation, the benchmarking results may reflect uneven edge for certain candidates, thereby undermining the fairness for the entire evaluation.

The LWC Hardware API After a period of public discussions, Kaps *et.al.* proposed the Hardware API for Lightweight Cryptography, commonly known as the LWC Hardware API [KDT+19], as specification of the compliance criteria, bus interface and communication protocol expected from the implementations submitted for hardware benchmarking of lightweight cryptography. The purpose of the API is to ensure uniformity of the implementations submitted, in terms of communications and a certain level of functionality. Only implementations compliant with this API will be considered in our benchmarking efforts.

Considered Candidates On May 7, 2020, we announced our intention to perform a study on ASIC benchmarking of the NIST lightweight candidates on the NIST lightweight cryptography forum. Since then, we have received 38 implementations of 10 candidates from 12 different design teams. All the 38 implementations are compliant with the LWC hardware API. The candidates considered are Ascon, DryGASCON, Elephant, Gimli, PHOTON-Beetle, Pyjamask, Romulus, Subterranean, TinyJAMBU and Xoodyak. Six submissions are submitted by the design teams of these candidates, namely Ascon, Gimli, Romulus, Subterranean, TinyJAMBU and Xoodyak (partenring with Silvia Mella). The implementation of DryGASCON was submitted by the independent designer Ekawat Homsirikamol. Five implementations are submitted by Kris Gaj from the GMU CERG team, namely Elephant, PHOTON-Beetle, Pyjamask, TinyJAMBU and Xoodyak. A summary of these implementations is given in Tables 1 and 2. All the implementations considered target only the primary AEAD variant of each candidate. In the rest of the report, add the suffix ‘cg’ when clock gating is applied during synthesis and ‘ncg’ otherwise.

Table 1: Candidates and implementations considered in this report.

Candidate	Architecture	Identifier	Language	Designer
Ascon	Basic iterative: 1-round	ascon-rp	vhdl	Robert Primas
DryGASCON	Basic iterative: 1-round	drygascon-eh	vhdl-verilog	Ekawat Homsirikamol
Elephant	Basic iterative: 1-round	elephant-rh-1	vhdl	Richard Haeussler
	Basic iterative: 5-round	elephant-rh-5	vhdl	Richard Haeussler
Gimli	Basic iterative: 1-round	gimli-pm-1	verilog	Pedro Maat Costa Massolino
	Basic iterative: 2-round	gimli-pm-2	verilog	Pedro Maat Costa Massolino
	Basic iterative: 3-round	gimli-pm-3	verilog	Pedro Maat Costa Massolino
	Basic iterative: 4-round	gimli-pm-4	verilog	Pedro Maat Costa Massolino
	Basic iterative: 6-round	gimli-pm-6	verilog	Pedro Maat Costa Massolino
	Basic iterative: 8-round	gimli-pm-8	verilog	Pedro Maat Costa Massolino
	Basic iterative: 12-round	gimli-pm-12	verilog	Pedro Maat Costa Massolino
PHOTON-Beetle	Basic iterative: 1-round	beetle-vl	vhdl	Vivian Ledynh
Pyjamask	Folded	pyjamask-rn-f	vhdl	Rishub Nagpal
	Pipelined	pyjamask-rn-p	vhdl	Rishub Nagpal
Romulus	Basic iterative: 1-round	romulus-mk-1	verilog-vhdl	Mustafa Khairallah
	Basic iterative: 2-round	romulus-mk-2	verilog-vhdl	Mustafa Khairallah
	Basic iterative: 4-round	romulus-mk-4	verilog-vhdl	Mustafa Khairallah
	Basic iterative: 8-round	romulus-mk-8	verilog-vhdl	Mustafa Khairallah
	Byte Sliding	romulus-mk-s	verilog-vhdl	Mustafa Khairallah

Table 2: Candidates and implementations considered in this report (Continued).

Candidate	Architecture	Identifier	Language	Designer
Subterranean	Basic iterative	subterranean-pm	verilog	Pedro Maat Costa Massolino
TinyJAMBU	Serial: 32-bit	tinyjambu-sl-32	vhdl	Sammy Lin
	Serial: 16-bit	tinyjambu-sl-16	vhdl	Sammy Lin
	Serial: 1-bit	tinyjambu-sl-1	vhdl	Sammy Lin
	Basic iterative: 8-round	tinyjambu-th-8	vhdl	Tao Huang
	Basic iterative: 32-round	tinyjambu-th-32	vhdl	Tao Huang
	Basic iterative: 128-round	tinyjambu-th-128	vhdl	Tao Huang
Xoodyak	Basic iterative: 1-round	xoodyak-sm-1	vhdl	Silvia Mella
	Basic iterative: 2-round	xoodyak-sm-2	vhdl	Silvia Mella
	Basic iterative: 3-round	xoodyak-sm-3	vhdl	Silvia Mella
	Basic iterative: 4-round	xoodyak-sm-4	vhdl	Silvia Mella
	Basic iterative: 6-round	xoodyak-sm-6	vhdl	Silvia Mella
	Basic iterative: 12-round	xoodyak-sm-12	vhdl	Silvia Mella
	Basic iterative: 1-round	xoodyak-rh-1	vhdl	Richard Haeussler
	Serial: 128-bit	xoodyak-rh-s	vhdl	Richard Haeussler

Use Cases In this report, we consider two use-cases for our initial study:

1. Performance Efficiency: We try to optimize the designs towards the best throughput/area ratio, by varying architectures, area and speed synthesis constraints. Once the optimization is done, extract different measurements for each architecture: area, power, throughput and energy.
2. Lightweight Protocols: We optimize the designs towards practical lightweight protocols. We choose two representative target protocols: Bluetooth and Bluetooth Low Energy (BLE). The application data rate of these protocols ranges between 0.27 and 2.1 Mbps, with an air data rate between 125 Kbps and 3 Mbps. Hence, we synthesize the designs for a target throughput of 3 Mbps for very long messages, and measure the corresponding area, power and energy.

In [BCL18], Burg *et.al.* provided a survey of the security needs of different wireless communication standard. They show that most relevant wireless communication protocols, with the exceptions of 802.11 variants, have data rates below 20 Mbps. The SigFox standard has a data rate of 100 bps and most of the standards have data rates in the Kbps range. However, our study shows that the power consumption and area of the circuit do not change significantly when the throughput is below the Mbps range. Hence, in order to simplify reading our reports, we consider the Bluetooth/BLE case with a target throughput of 3 Mbps, assuming the area and power consumption is almost constant below such rate and the energy varies linearly with the data rate. This is due to the fact that at such frequencies, the power consumption is dominated by the static power that does not depend on the frequency. The same is not true for high data rates as they can affect the area and power consumption significantly and non-linearly, as the switching power depends on the target frequency, while the synthesizer may require larger, more power consuming standard cells to achieve such high data rates. For 802.11 and other applications that require high data rates, we introduce the first use case.

Process and Flow For this study, we used an area-oriented and throughput-oriented synthesis flow, given in Figure 1. We used the Synopsys VCS K-2015.09SP2-10 and Xilinx ISIM 14.7 simulators, and the Synopsys Design Compiler Q-2019-12-SP5. We used the general-purpose industry grade TSMC TSBN 65nm 9-track standard cell library as a target. We used Python for generating and analyzing the results. The simulation is used to generate the data useful to the analyze the synthesis outputs, namely throughput and energy.

Data Size In accordance with the FPGA benchmarking project by the CERG team, we consider 9 different data sizes:

1. 16 bytes of associated data.
2. 64 bytes of associated data.
3. 1536 bytes of associated data.
4. 16 bytes of plaintext.
5. 64 bytes of plaintext.
6. 1536 bytes of plaintext.
7. 16 bytes of both associated data and plaintext.
8. 64 bytes of both associated data and plaintext.

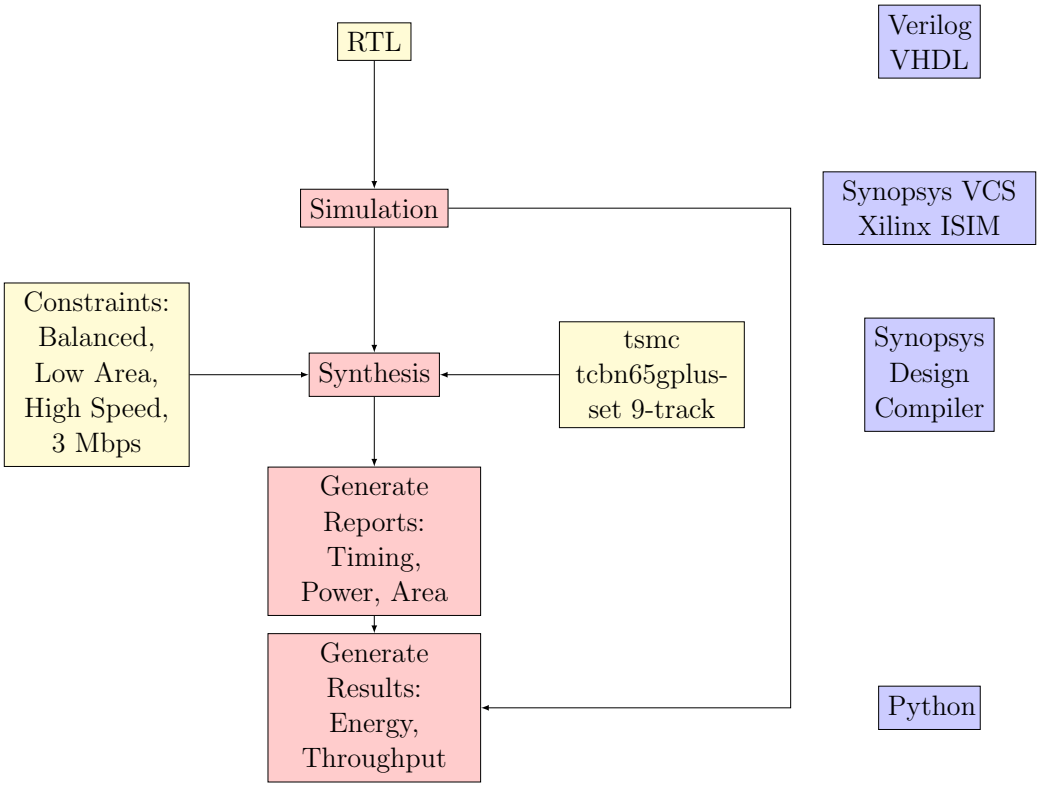

Figure 1: The synthesis flow and tools used for our Study.

9. 1536 bytes of both associated data and plaintext.

1536 Bytes is the size of the Maximum Transmission Unit (MTU) of Ethernet [eth]. Besides, the IETF IMIX GENOME defines benchmarking packets for internet applications that start from 64 bytes [imi]. It is expected that lightweight protocol can have even smaller packets. Given these data sizes, we cover both short messages and relatively long messages. We can also assess the cost of authentication vs. encryption.

2 Limitations and goals

The task of fairly comparing 10 or more different algorithms in a short time span is not straightforward. One may think of different goals for such process:

1. Compare the baseline performance of different algorithms.
2. Optimize different algorithms.
3. Rank different algorithms.
4. Compare the optimized performance of different algorithms.

While all these are valid goals, the delays in the process of developing the RTL code, the number of designs, due to the ongoing COVID-19 pandemic and the time constraints of the standardization process imposes additional constraints. Hence, we opt for a two phase approach:

1. Design space exploration: during round 2 of the standardization process, we study 10 candidates in terms of front-end design (synthesis). While this approach has the side-effect of reducing the accuracy, it is usually used in the early stages of design exploration to quickly compare many implementations and designs. This gives us an idea on what to expect from each design.

2. Optimization: during round 3 of the standardization process, we should be able to look more in depth on the back-end design of the finalists (layout). The NIST team announced they expect 8 finalists. Hopefully, the data obtained in this report will help us in round 3 to go deeper in the analysis with more time span.

Another limitation of our study is that the implementations are done by several teams with varying optimization level and code quality. One way to overcome this is to take a deeper look at optimizing the implementations and/or work with the designers to find better architectures.

3 Summary and Rankings

Given the results in this report, we rank the candidates considered according to their best result in different metrics. We provide two types of rankings. The first one is general rankings based on different metrics, represented as a bar chart. For example, Figure 2 shows the energy×area ranking for 16-byte messages on the TSMC 65nm library. The length of each bar is proportional to the minimum energy×area value that each design gets. Consequently, the graph does not only show the rank of each design, but also how close it is to its neighbors. It can be seen that in Figure 2 TinyJAMBU and Subterannean are close, while Ascon, Xoodyak and DryGASCON are close, with Romulus filling the gap between the two groups. Such ranking figures are given for energy×area, energy and area in Figures 2 to 15, where a lower rank is better. In this figures we excluded Pyjamask as its implementation is an outlier, being both very slow and very big. The second type of ranking is ranking the designs with a moving area threshold. We look at how the implementations rank when we move the area constraint from 5 kGE all the way up to 50 kGE. For example, some designs may offer a speed-area trade-off by using many architectures, and some designs can over high speed implementations but they cannot fit in a tightly constrained environment, or, on the other hand, offer very small implementation but their speed does not scale by increasing the area. In Figures 16 to 33 show such moving rankings, where the x-axis represent the area threshold ('O' is the ranking for very large area), and the y-axis shows the order to different designs that can fit within such constraint. In this case, the higher the rank, the better. A summary of different rankings is given in Table 3. However, these rankings should be understood as a very tiny glimpse at the big picture that follows in the report.

4 Raw Synthesis Results

In this section, we report the raw synthesis results for the implementations considered. Each implementation is synthesized against four different corner cases: balanced (BC), low-area (LA), high-speed (HS) and low frequency (LF) targetting ∼3 Mbps throughput. The results reported are area in both μm^2 and gate equivalents (GE), clock period in ns and power in mW. The results for TSMC 65nm (using CCS circuit models) are shown in Tables 4, 5, 6, 7, 8, 9, 10, 11, 12 , 13 and 14, while the results for FDSOI 28nm are shown in Tables 15, 16, 17, 18, 19, 20, 21, 22, 23 , 24 and 25. For simplicity, the xoodyak-rh-* implementations of Xoodyak are excluded as they either presents a anomaly in the results (both slow and large in terms of area) or almost the same as other included implementations.

Table 3: Summarized Rankings of Different Designs.

Scheme	$E \times A$	E	T	A	$E \times A$ (3 Mbps)	E (3 Mbps)
Subterannean	1	1	1	3	3	4
TinyJAMBU	2	2	7	1	1	1
Romulus	3	4=	3=	2	2	2
Gimli	4=	3	3=	7	6	6
Xoodyak	4=	4=	2	4	5	5
Ascon	6	6=	3=	6	4	3
DryGASCON	7	6=	6	9	9	8
PHOTON-Beetle	8	8=	8=	8	8	7
Elephant	9	8=	8=	5	7	9
Pyjamask	10	10	10	10	10	10

We believe this is due to the use of large register files that maybe cheap in FPGAs but not suitable for ASIC.

5 Energy×Area

The energy×area comparison metric represents the main trade-off that the designer for a constrained environment is faced with. On one hand, the designer wants to minimize the time required to process a certain amount of data, *i.e.*, the latency. On the other hand, the designer needs to reduce the cost spent to perform the computation. The cost consist of mainly two components: manufacturing cost, *i.e.*, area, and running cost, *i.e.*, power consumption. Hence, the designer's goal is to minimize the cost function given by

$$L \times P \times A$$

where L is the latency, P is the power consumption, and A is the circuit area. $L \times P$ can be rewritten as energy E. Hence, the cost function becomes

$$E \times A$$

The minimum energy×area implementation for each design is given in Tables 26, 28 and 30 for TSMC 65nm and Tables 27, 29 and 31 for FDSOI 28nm.

6 Energy

In devices where the main constraint comes from the usage of a battery, the longevity of such battery, and cosnequently the energy consumption becomes the primary goal of the designer. Tables 32, 34 and 32 give the estimated energy consumption on TSMC 65nm needed in order to process messages of 16 bytes, 64 bytes and 1536 bytes, respectively, while Tables 33, 35 and 33 give the estimated energy consumption on FDSOI 28nm. |A| and |M| refers to the size of associated data and plaintext in bytes, respectively. AD cost refers to the energy overhead when encrypting X bytes of plaintext and X bytes of associated data vs. only X bytes of plaintext, with 0.00 being the lowest.

7 Throughput

In high performance applications, cost is less important compared to speed. Hence, throughput becomes the main decision factor. However, the cost has to remain within

reasonable bounds. Given the different corner cases with the aid of simulation outputs, we get the throughput for different message sizes. Tables 38, 40 and 42 include the maximum achievable throughput on TSMC 65nm for 16 bytes, 64 bytes and 1536 bytes, respectively, for reasonably low power. In other words, we focus on the BC and LA corners. While some designs can achieve higher throughputs using the HS corner, this comes at the expense of unreasonable power consumption. Hence, we leave it for interested readers to find the throughput at the HS corner by multiplying the throughput by CP[HS]/CP[BC] or CP[HS]/CP[LA], where CP[X] is the clock period at corner X. Such high power consumption is not suitable for lightweight devices and not suitable for ranking the designs. Tables 39, 41 and 43 include the maximum achievable throughput on FDSOI 28nm for 16 bytes, 64 bytes and 1536 bytes, respectively, for reasonably low power. |A| and |M| refers to the size of associated data and plaintext in bytes, respectively. AD efficiency refers to the gain in throughput when encrypting X bytes of plaintext and X bytes of associated data vs. only X bytes of plaintext, with 1.00 being the highest.

8 Trade-offs

In the Figures 52 to 139, we give a more fine-grained look at the different speed, power, area and energy trade-offs for different designs, for different message length, for both high speed applications, *i.e.*, the performance efficiency use case and the lightweight protocols use case.

9 Conclusions

The results in this report give an idea about the ASIC performance of 10 round 2 candidates for the NIST lightweight cryptography competition: Ascon, DryGASCON, Elephant, Gimli, PHOTON-Beetle, Pyjamask, Romulus, Subterranean, TinyJAMBU and Xoodyak. We study different performance metrics and trade-offs, across two use cases: performance efficiency and Bluetooth communication. The results show that some algorithms behave differently in different use cases, while others maintain a somewhat uniform profile across different metrics. For example, the results show that Pyjamask does not fare well when it comes to unprotected hardware implementations, ranking last in most metrics, and in most cases with a big margin. Subterranean ranks first in most metrics except when it comes to low data rates. A group of 5 candidates: Ascon, Gimli, Romulus, TinyJAMBU and Xoodyak trade rankings below Subteranneanean, with Romulus and TinyJAMBU more biased towards low area, short messages and overall efficiency (energy×area), while Ascon, Gimli and Xoodyak rank better in terms of pure speed. DryGASCON is close to the bottom of this group but it notably ranks better on FDSOI 28nm than it does on TSMC 65nm. The next group is Elephant and PHOTON-Beetle, while Pyjamask ranks last (with big margin) in most categories. On the other hand, only two designs (Romulus and TinyJAMBU) achieve notable results with area below 6 kGE, which place them in top two in terms of minimum Area. Four designs achieve results with less than 9kGE, with Subterranean and Xoodyak joining the pack.

What does this mean? The benchmarking of different candidates only measures the corresponding implementations submitted. Hence, it is not a definitive answer to the optimal performance and potential of every candidate as it is likely that novel optimizations can be found. However, it measures the state-of-the-art of implementations. Designers are encouraged to find spots where their implementations are not optimal and enhance it accordingly.

Acknowledgment

We would like to thank Kris Gaj, Mark Aagard, and Pedro Maat Costa Massolino for their inputs and insights on the ASIC benchmarking. We would like to also thank the designers of the LWC Hardware API for their efforts that made this benchmarking process possible.

References

[BCL18] A. Burg, A. Chattopadhyay, and K. Lam. Wireless communication and security issues for cyber–physical systems and the internet-of-things. *Proceedings of the IEEE*, 106(1):38–60, 2018. https://ieeexplore.ieee.org/abstract/document/8232533.

[BL20] Daniel J. Bernstein and Tanja Lange. eBACS: ECRYPT Benchmarking of Cryptographic Systems. https://bench.cr.yp.to/supercop.html, 2020.

[CAE20] CAESAR Competition. CAESAR submissions. https://competitions.cr.yp.to/caesar-submissions.html, 2020.

[eth] Extended ethernet frame size support.

[imi] Imix genome: Specification of variable packet sizes for additional testing.

[KDT+19] Jens-Peter Kaps, William Diehl, Michael Tempelmeier, Ekawat Homsirikamol, and Kris Gaj. Hardware API for Lightweight Cryptography. 2019.

[KHYKC17] Sachin Kumar, Jawad Haj-Yihia, Mustafa Khairallah, and Anupam Chattopadhyay. A Comprehensive Performance Analysis of Hardware Implementations of CAESAR Candidates. *IACR Cryptology ePrint Archive, Report 2017/1261*, 2017. https://eprint.iacr.org/2017/1261.pdf.

[MHN+20] Kamyar Mohajerani, Richard Haeussler, Rishub Nagpal, Farnoud Farahmand, Abubakr Abdulgadir, Jens-Peter Kaps, and Kris Gaj. Fpga benchmarking of round 2 candidates in the nist lightweight cryptography standardization process: Methodology, metrics, tools, and results. Cryptology ePrint Archive, Report 2020/1207, 2020. https://eprint.iacr.org/2020/1207.

[NIS18] NIST. Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process, 2018. https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/final-lwc-submission-requirements-august2018.pdf.

[SR20] Jürgen Mottok Sebastian Renner, Enrico Pozzobon. NIST LWC Software Performance Benchmarks on Microcontrollers. https://lwc.las3.de/, 2020.

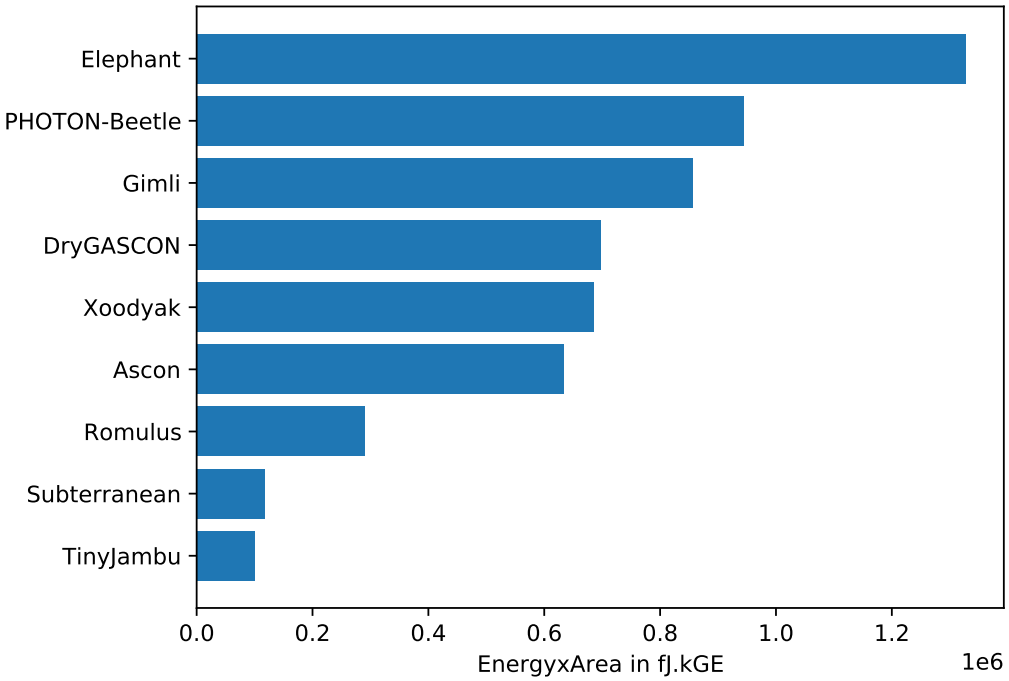

Figure 2: Energy×Area ranking for 16-byte messages on TSMC 65nm.

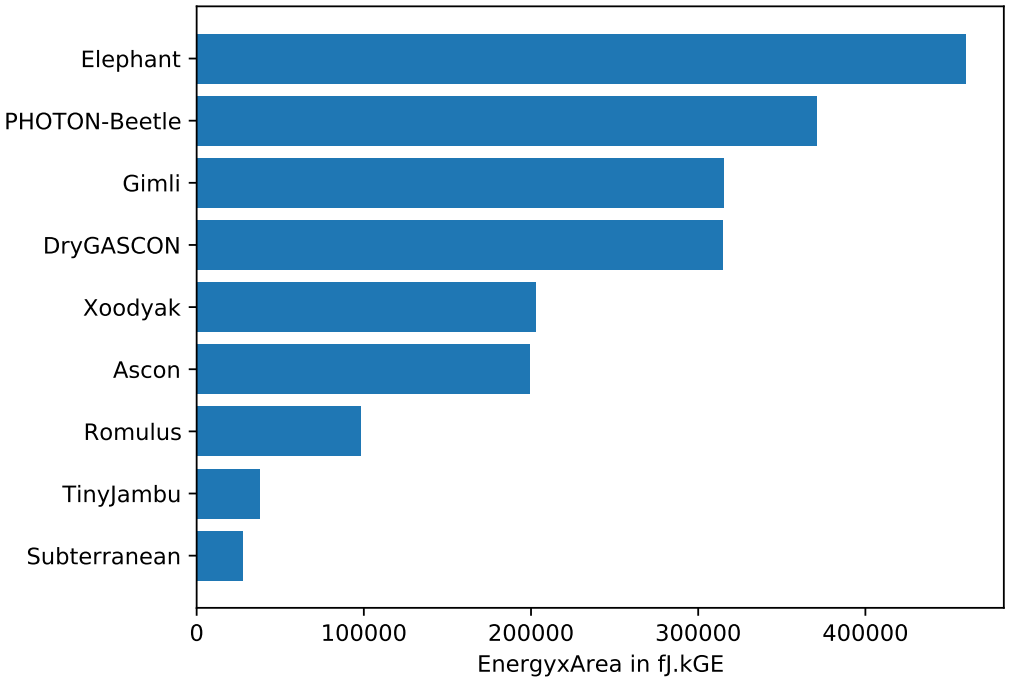

Figure 3: Energy×Area ranking for 16-byte messages on FDSOI 28nm.

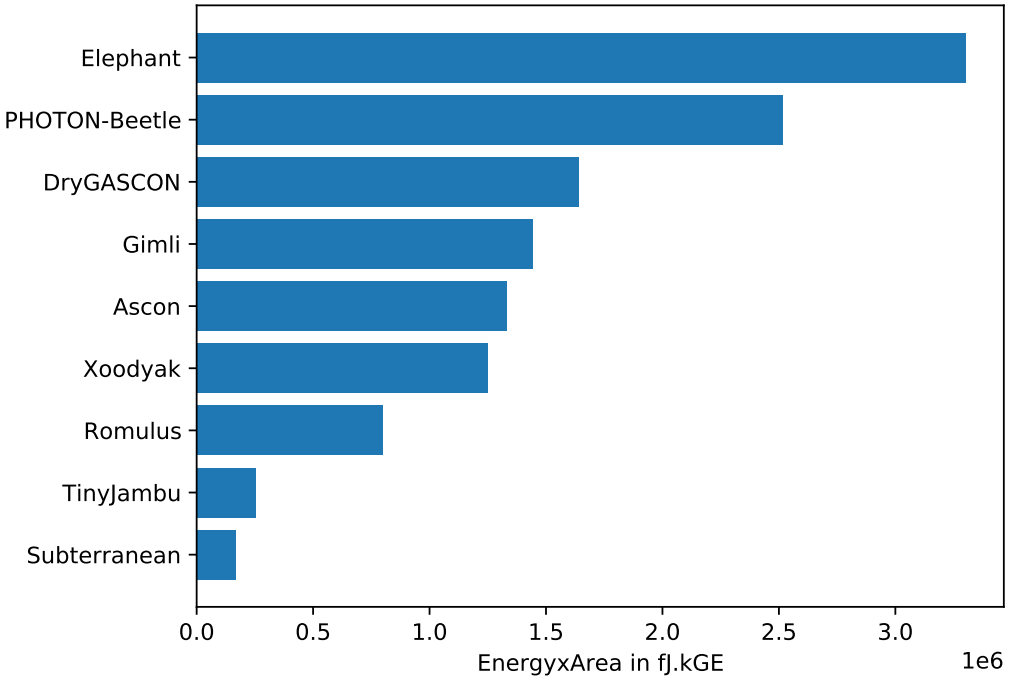

Figure 4: Energy×Area ranking for 64-byte messages on TSMC 65nm.

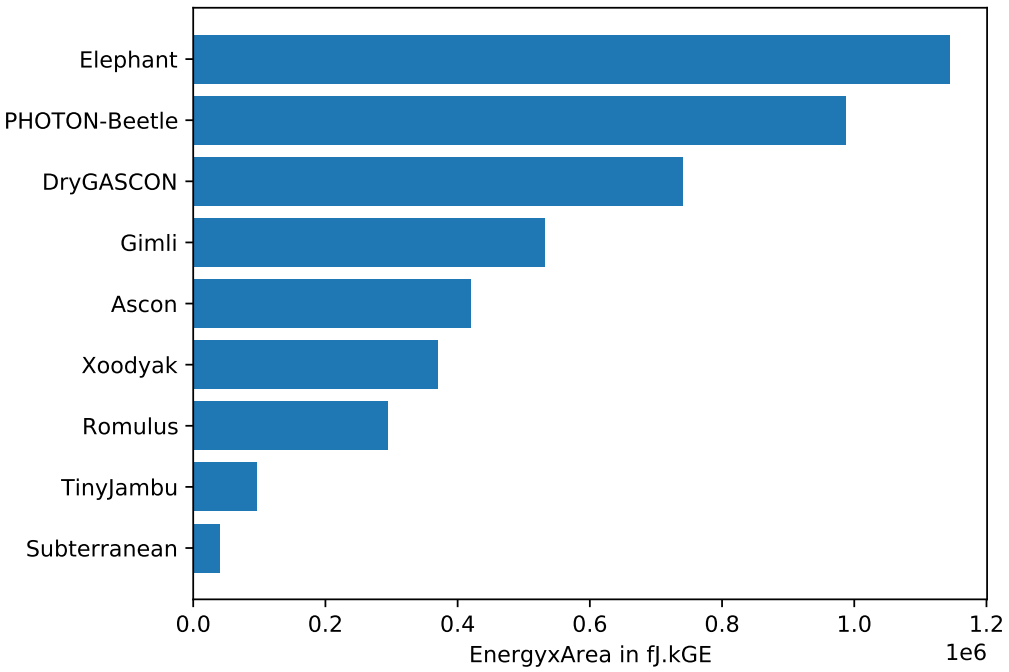

Figure 5: Energy×Area ranking for 64-byte messages on FDSOI 28nm.

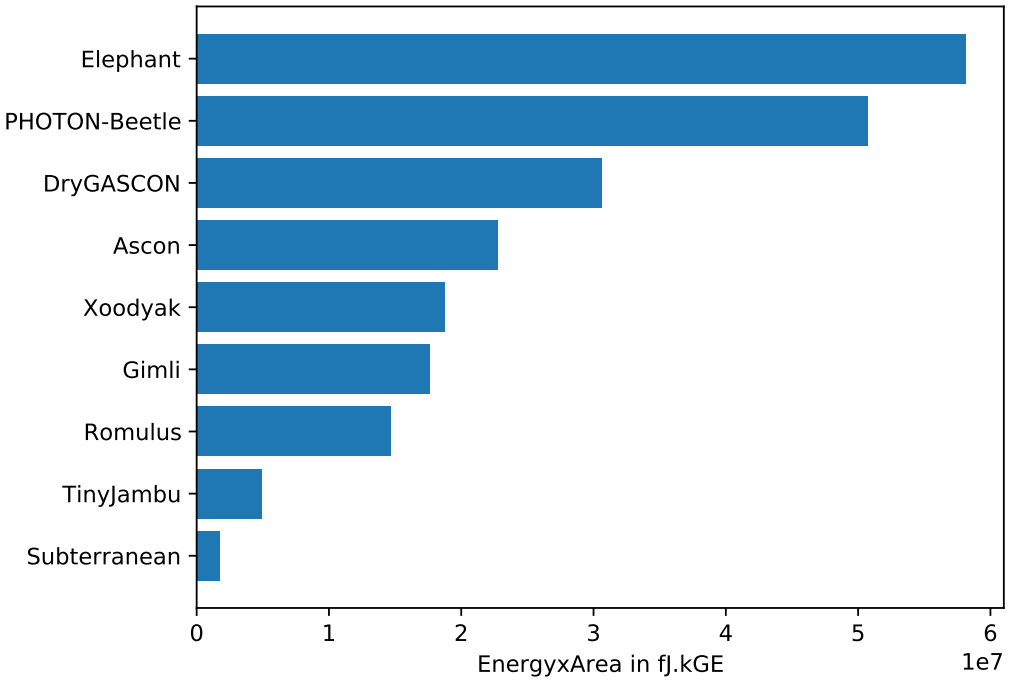

Figure 6: Energy×Area ranking for 1536-byte messages on TSMC 65nm.

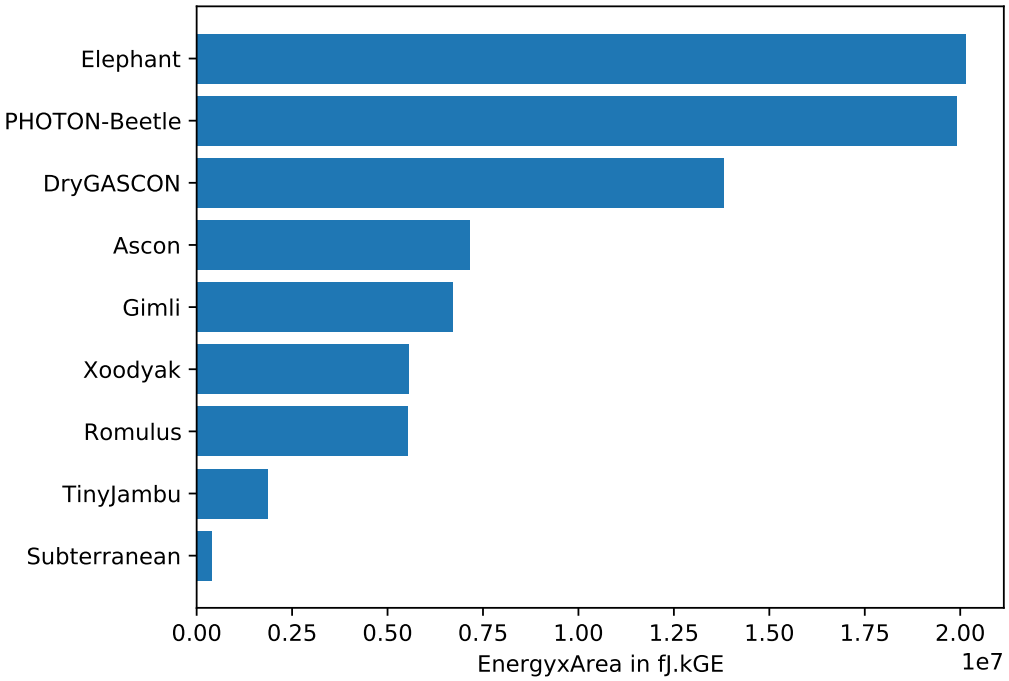

Figure 7: Energy×Area ranking for 1536-byte messages on FDSOI 28nm.

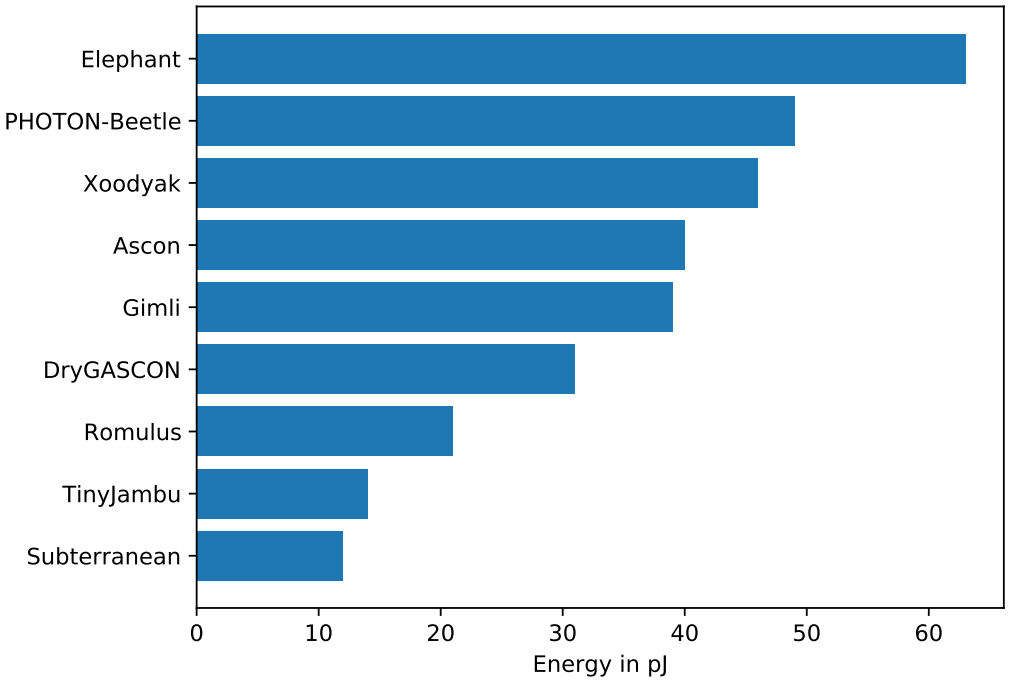

Figure 8: Energy ranking for 16-byte messages on TSMC 65nm.

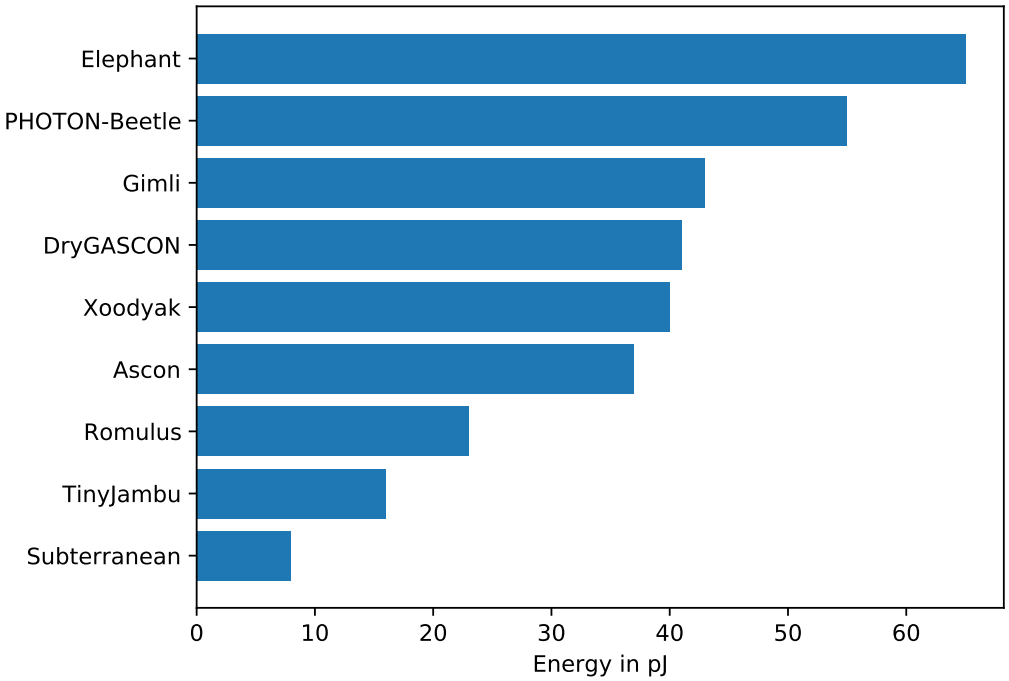

Figure 9: Energy ranking for 16-byte messages on FDSOI 28nm.

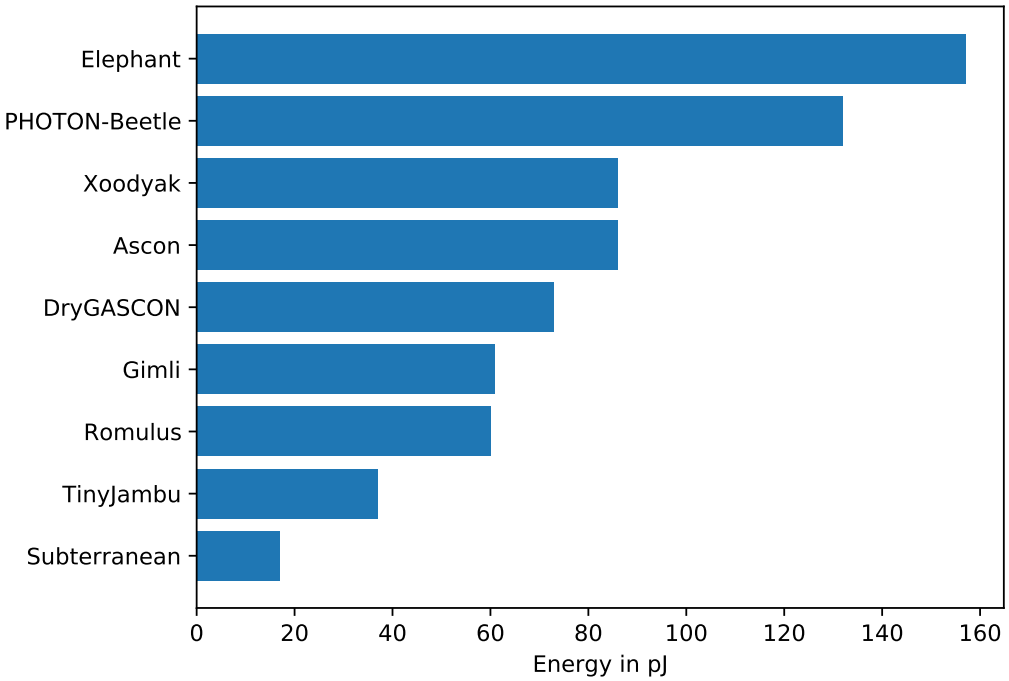

Figure 10: Energy ranking for 64-byte messages on TSMC 65nm.

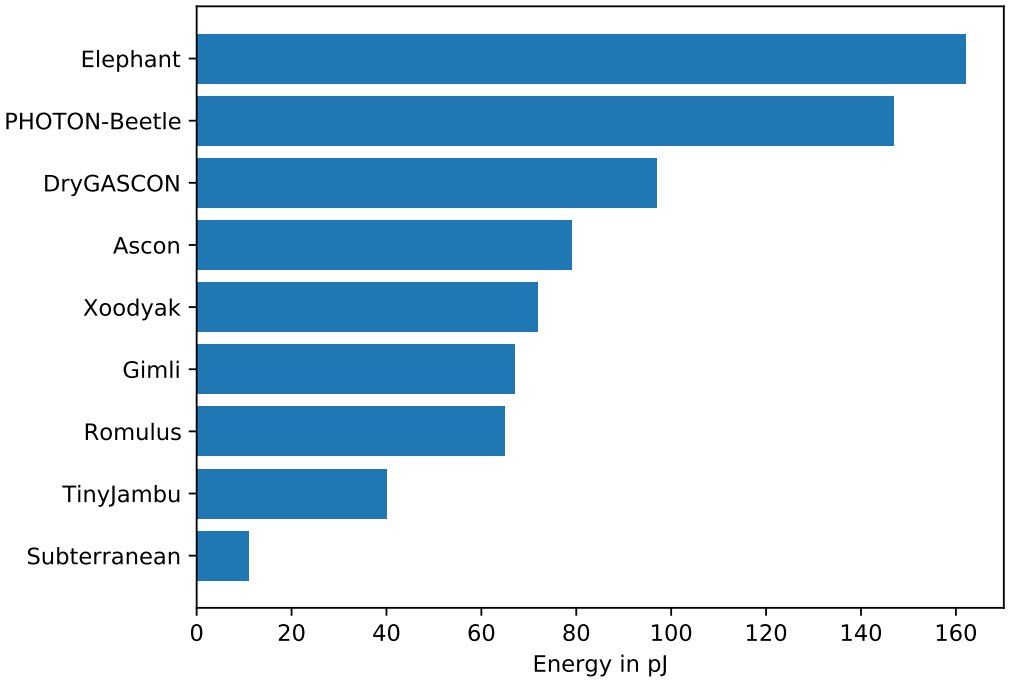

Figure 11: Energy ranking for 64-byte messages on FDSOI 28nm.

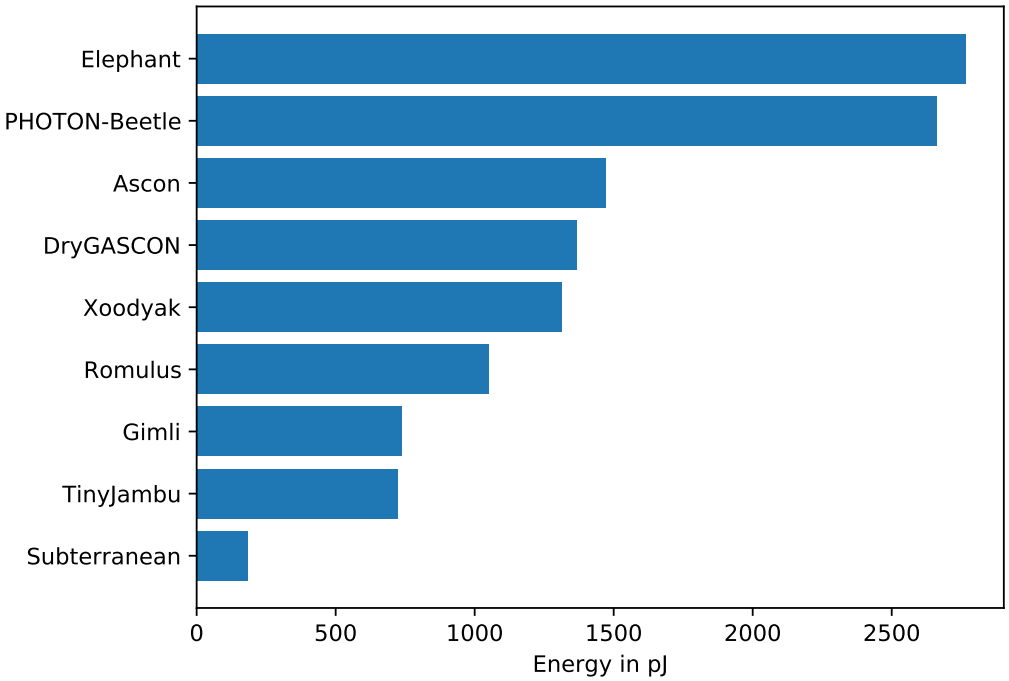

Figure 12: Energy ranking for 1536-byte messages on TSMC 65nm.

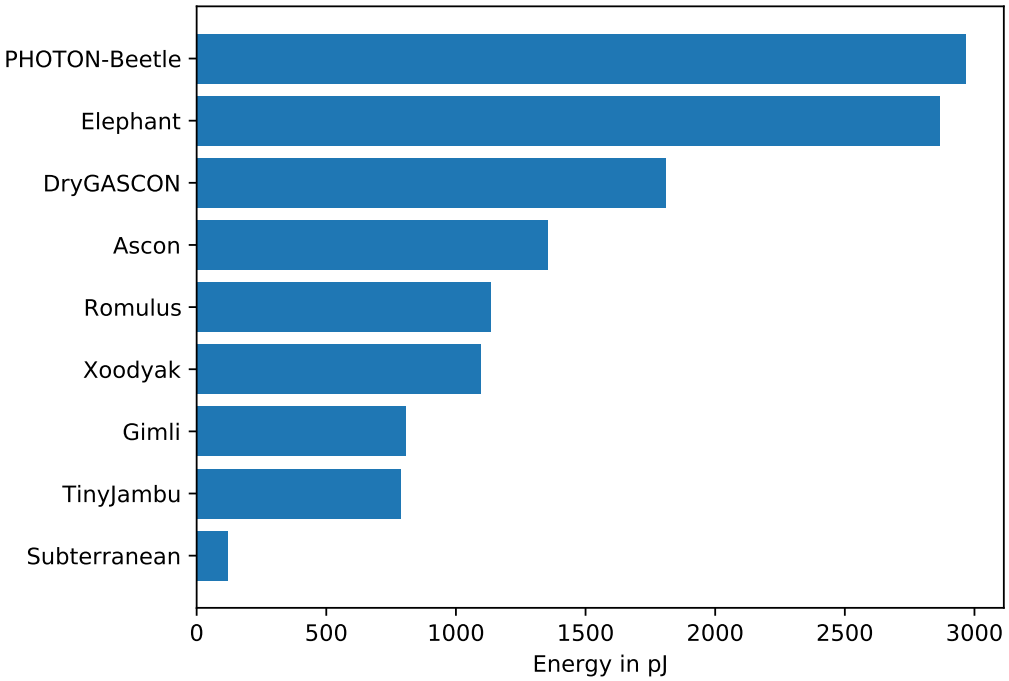

Figure 13: Energy ranking for 1536-byte messages on FDSOI 28nm.

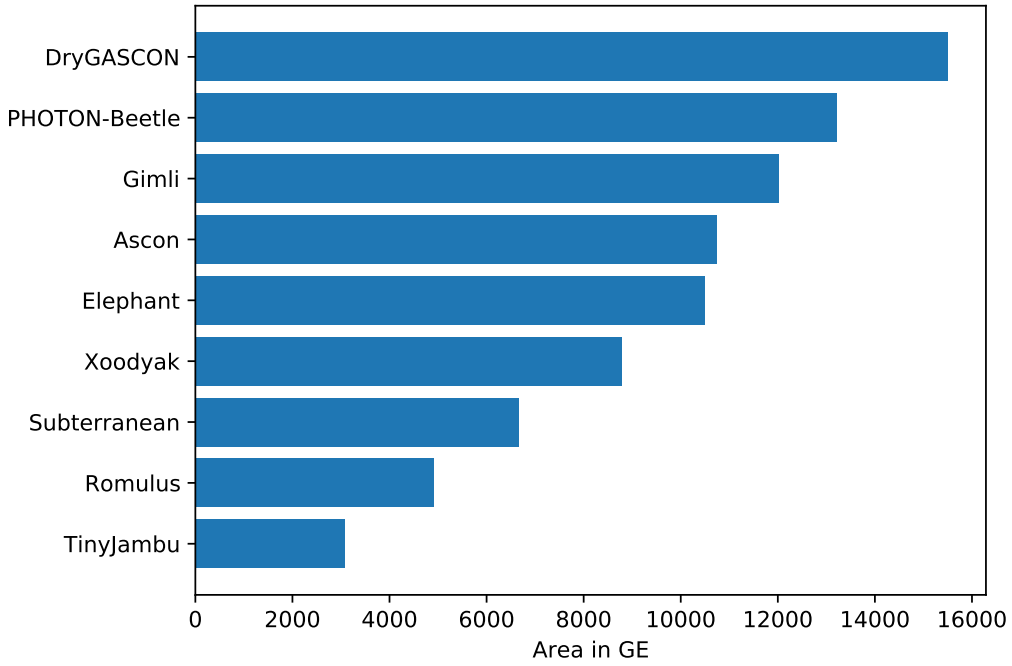

Figure 14: Area ranking on TSMC 65nm.

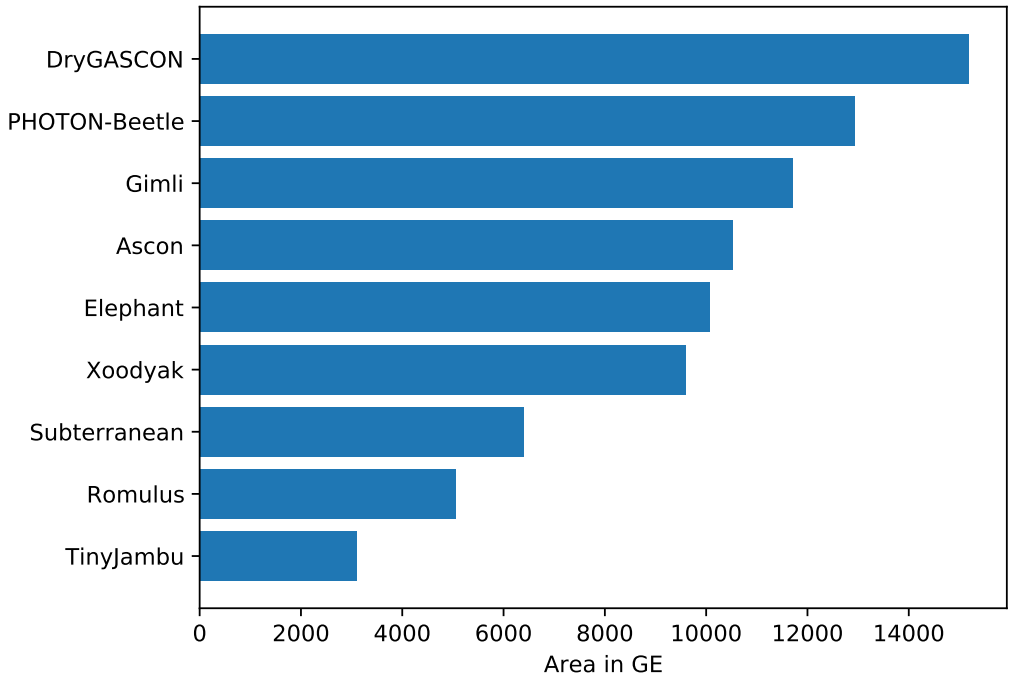

Figure 15: Area ranking on FDSOI 28nm.

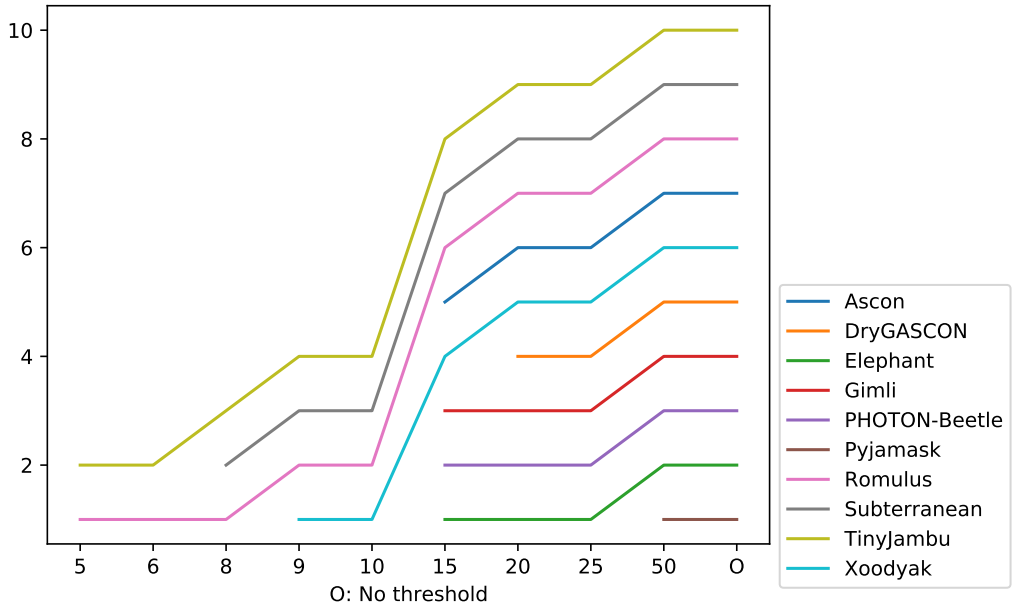

Figure 16: Energy×Area moving ranking for 16-byte messages on TSMC 65nm.

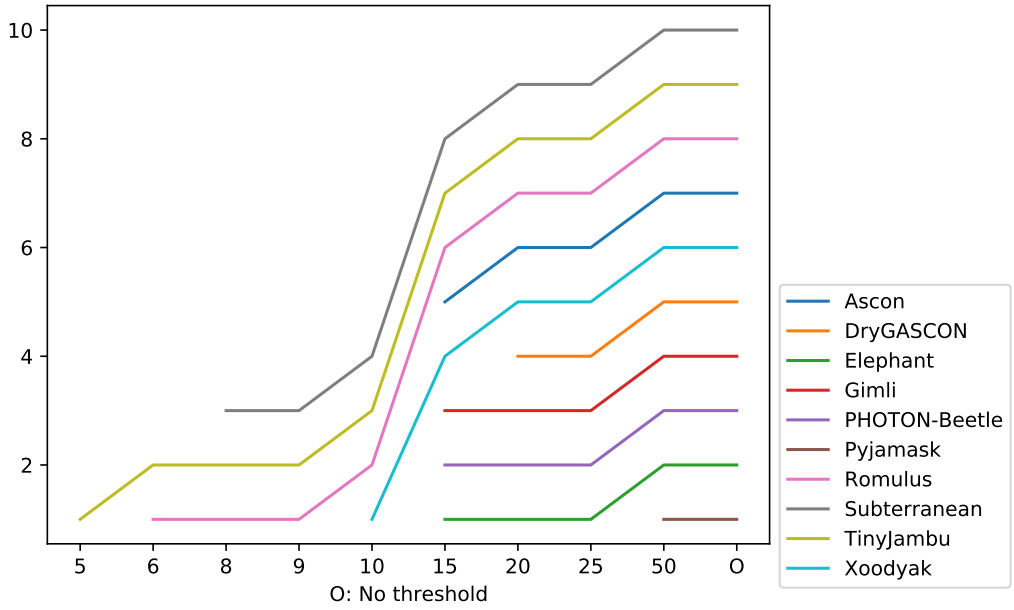

Figure 17: Energy×Area moving ranking for 16-byte messages on FDSOI 28nm.

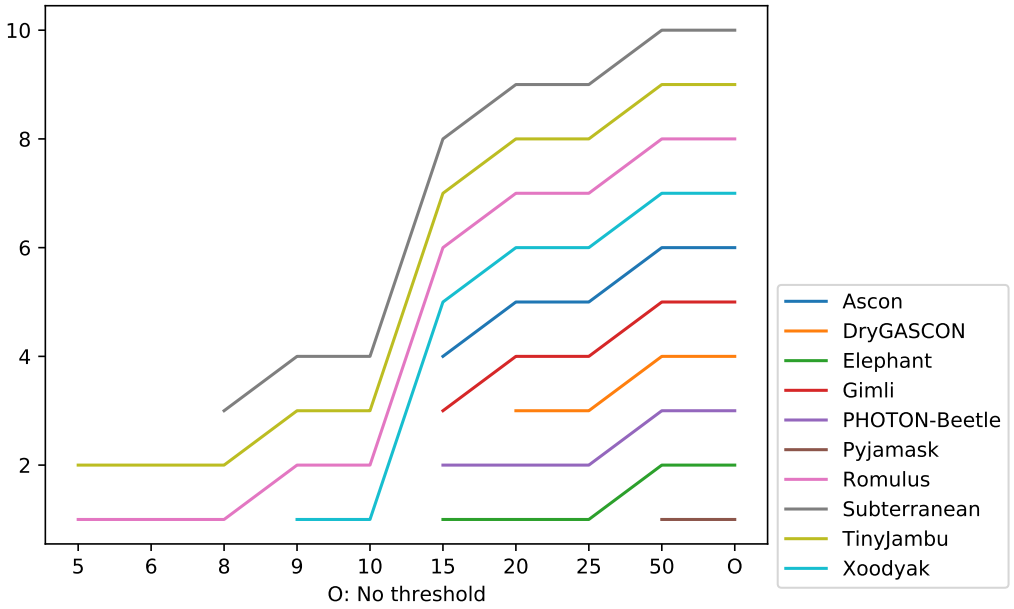

Figure 18: Energy×Area moving ranking for 64-byte messages on TSMC 65nm.

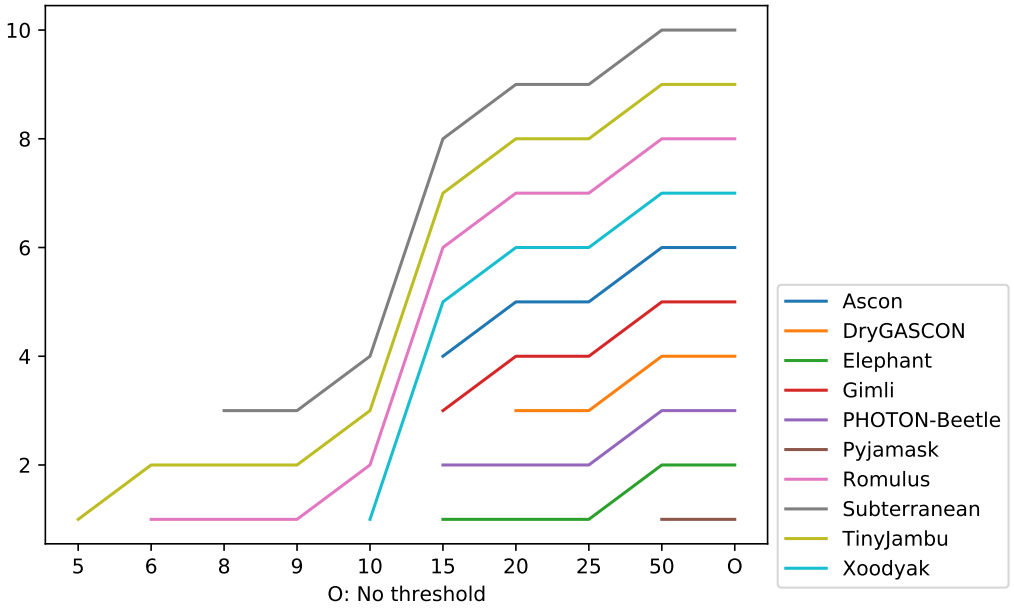

Figure 19: Energy×Area moving ranking for 64-byte messages on FDSOI 28nm.

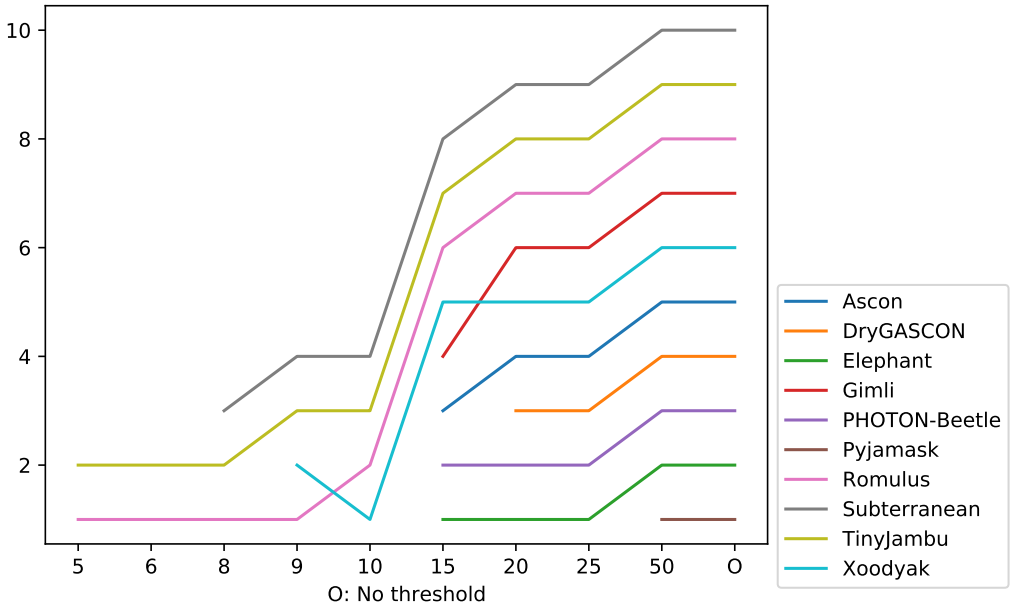

Figure 20: Energy×Area moving ranking for 1536-byte messages on TSMC 65nm.

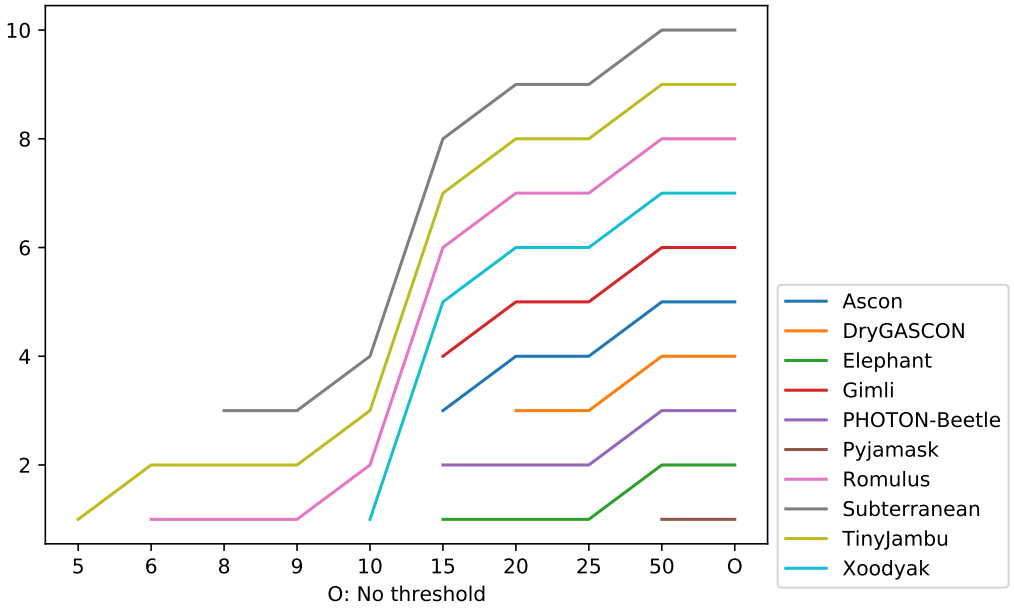

Figure 21: Energy×Area moving ranking for 1536-byte messages on FDSOI 28nm.

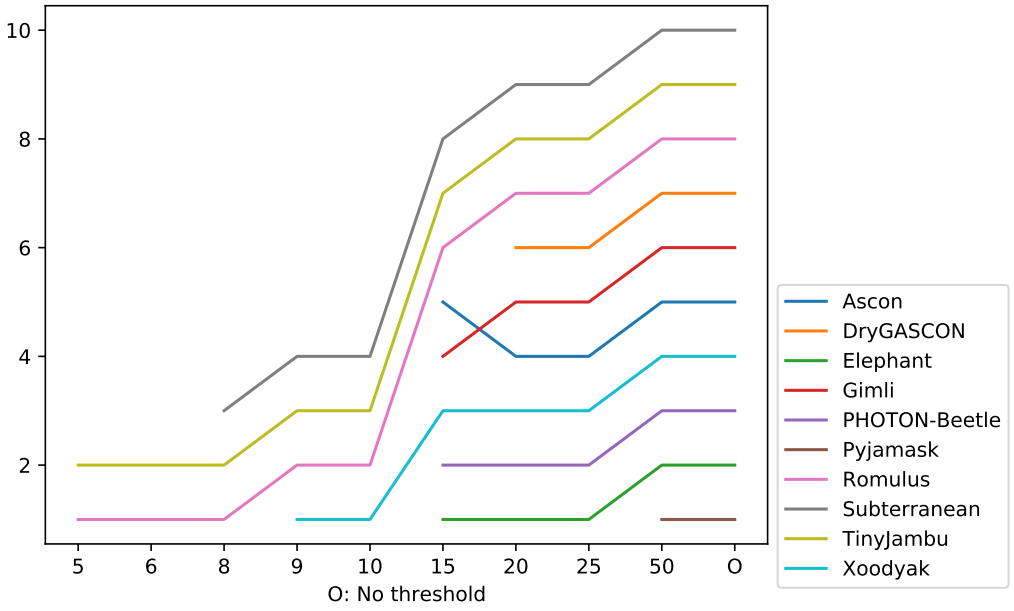

Figure 22: Energy moving ranking for 16-byte messages on TSMC 65nm.

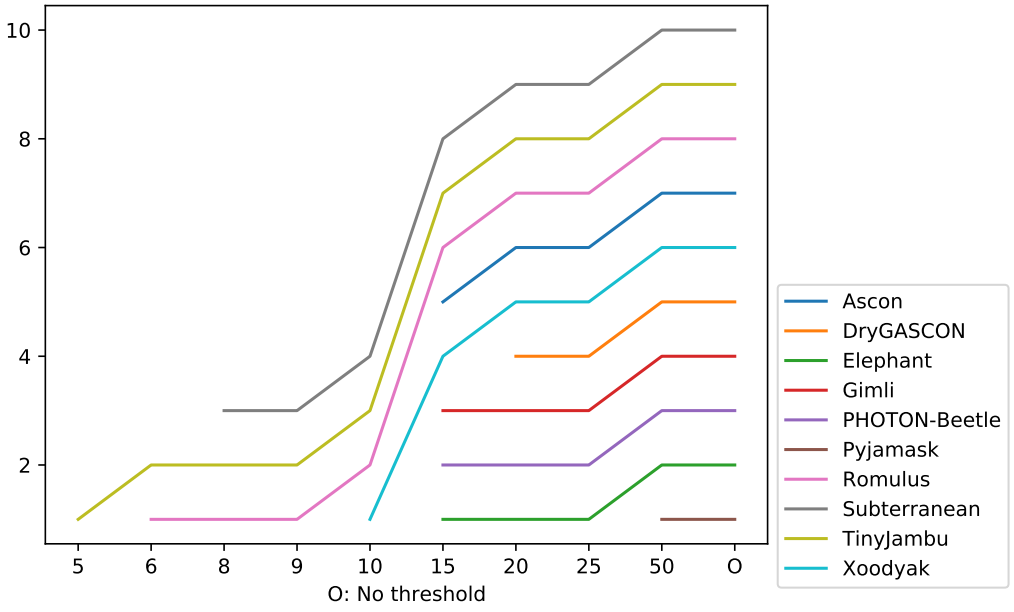

Figure 23: Energy moving ranking for 16-byte messages on FDSOI 28nm.

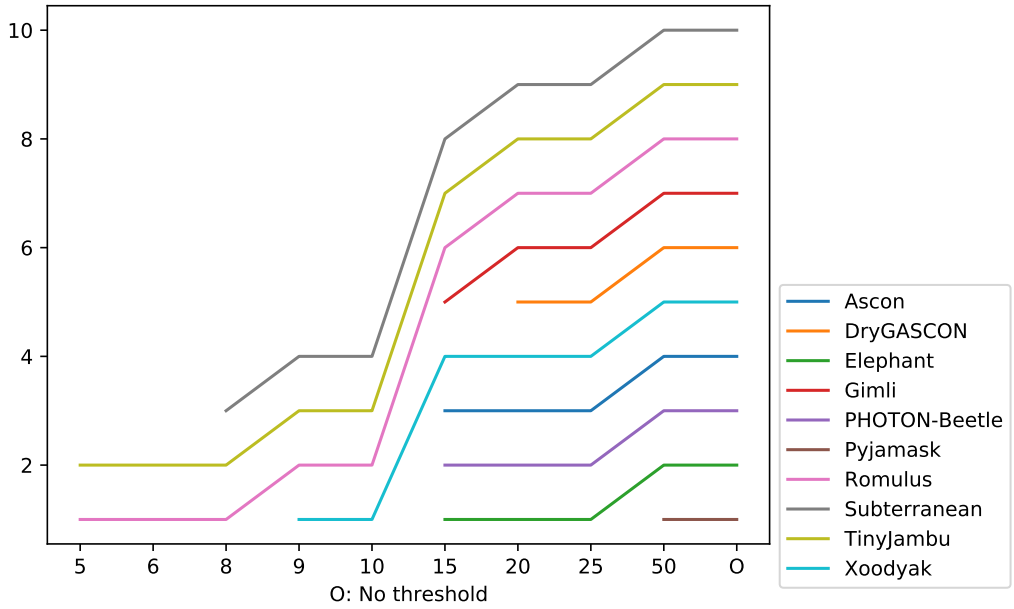

Figure 24: Energy moving ranking for 64-byte messages on TSMC 65nm.

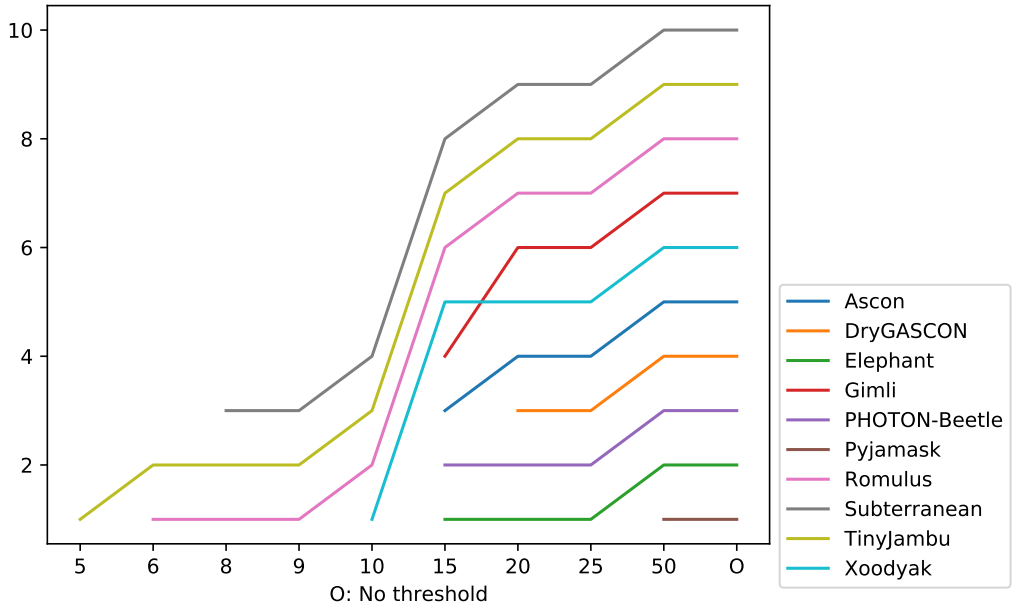

Figure 25: Energy moving ranking for 64-byte messages on FDSOI 28nm.

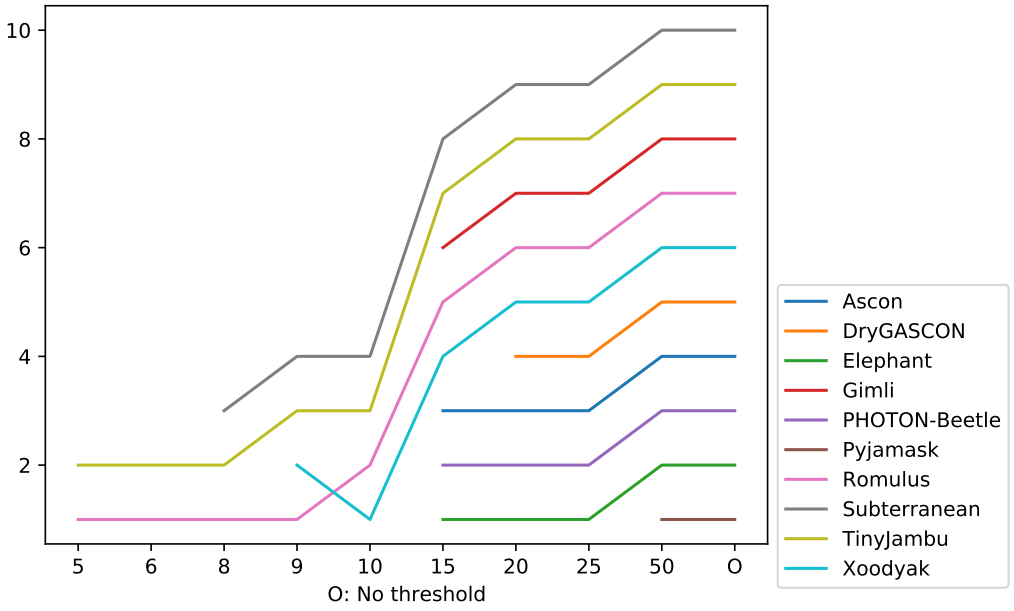

Figure 26: Energy moving ranking for 1536-byte messages on TSMC 65nm.

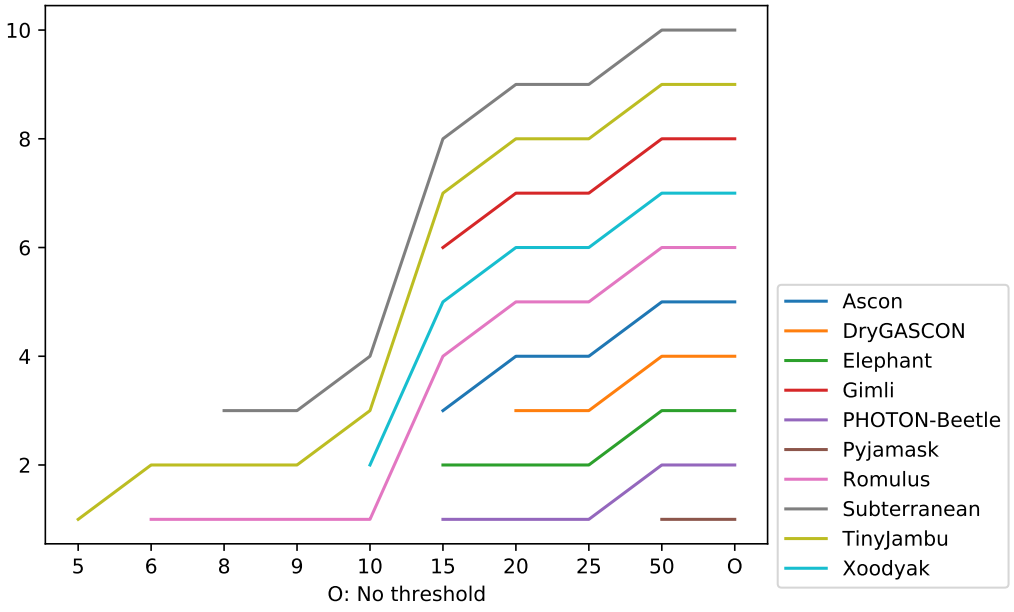

Figure 27: Energy moving ranking for 1536-byte messages on FDSOI 28nm.

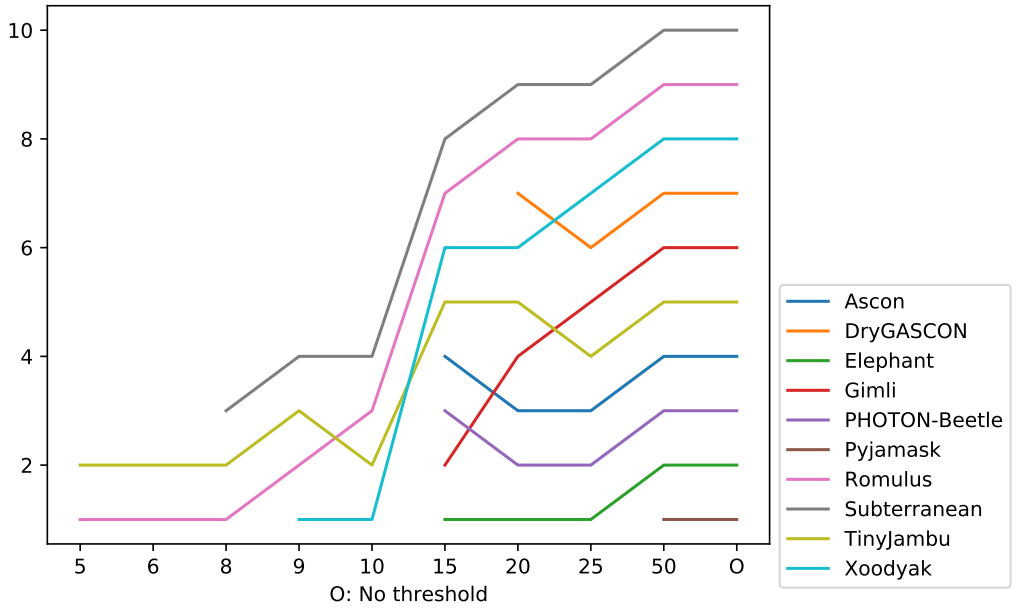

Figure 28: Throughput moving ranking for 16-byte messages on TSMC 65nm.

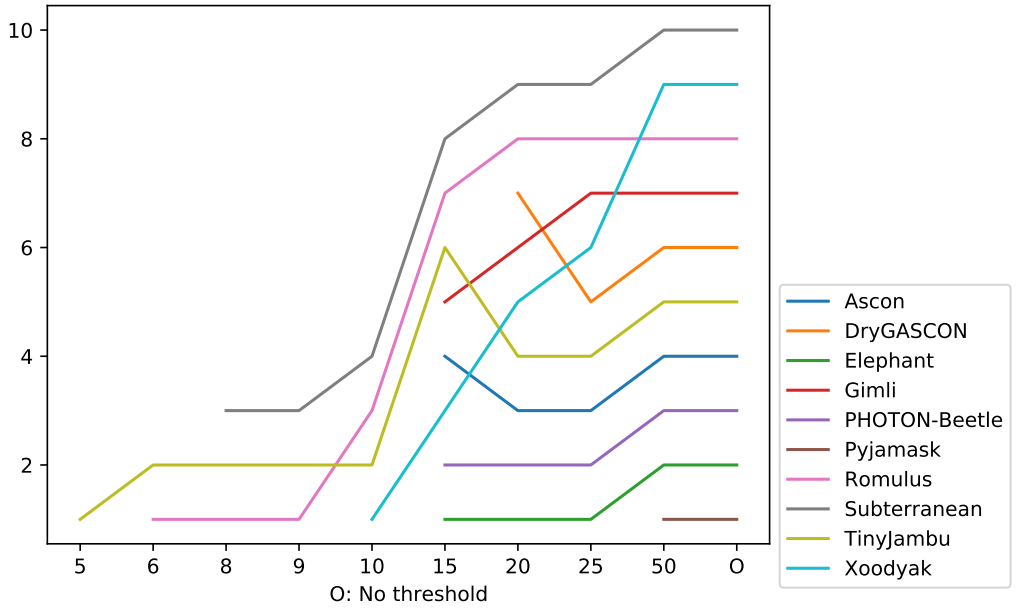

Figure 29: Throughput moving ranking for 16-byte messages on FDSOI 28nm.

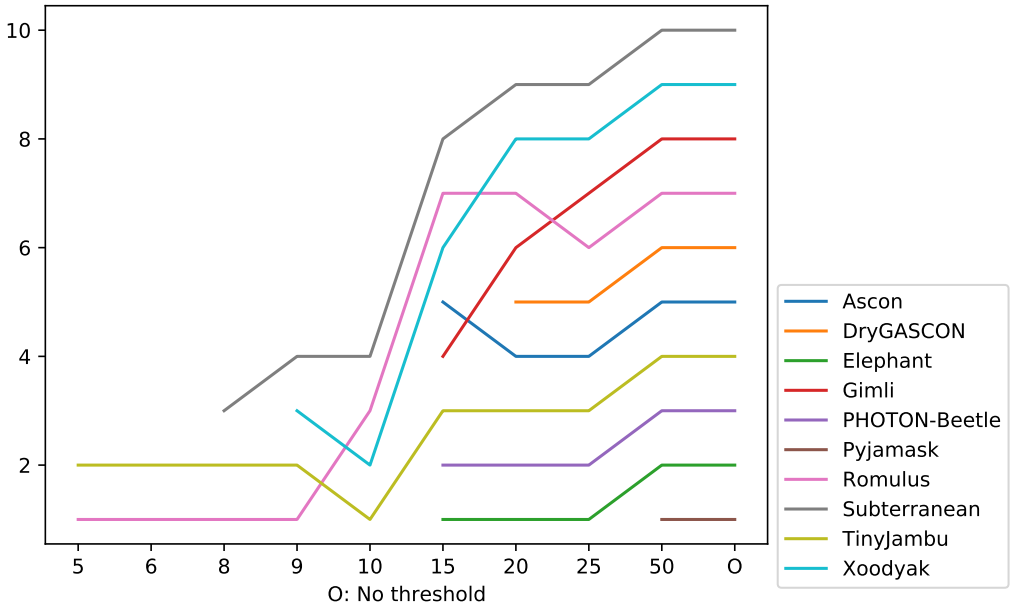

Figure 30: Throughput moving ranking for 64-byte messages on TSMC 65nm.

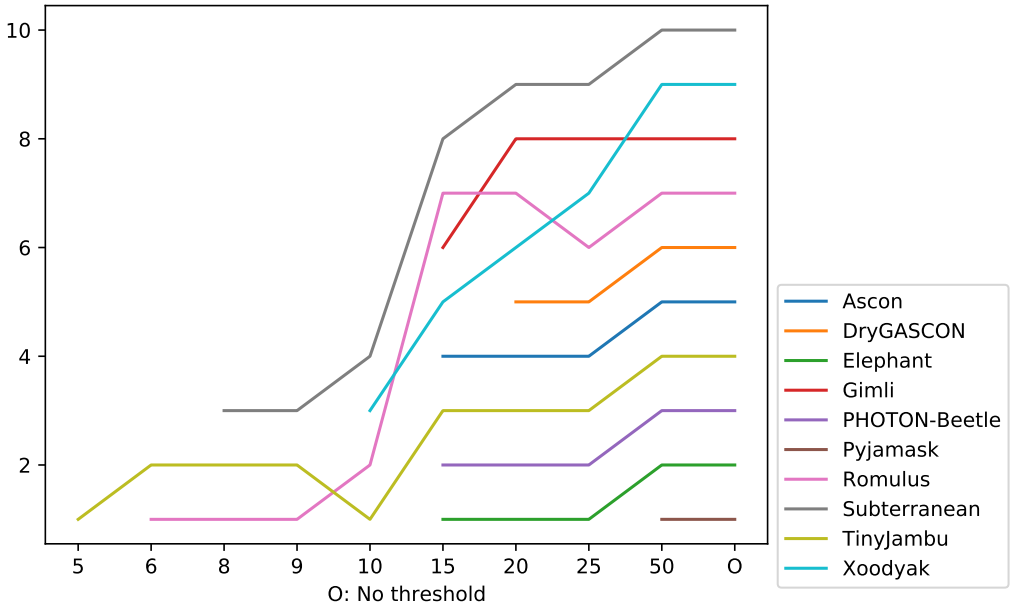

Figure 31: Throughput moving ranking for 64-byte messages on FDSOI 28nm.

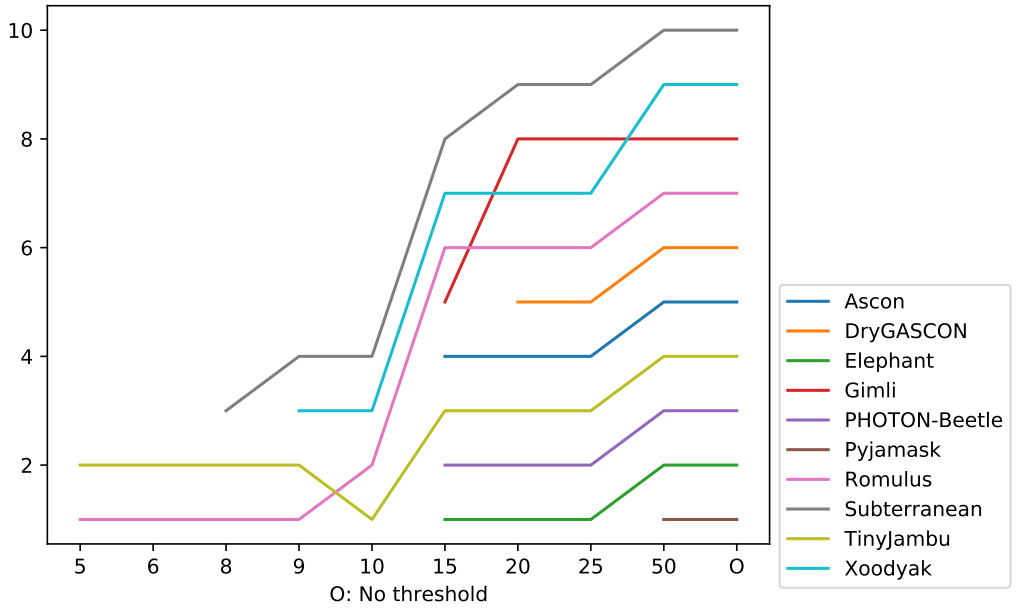

Figure 32: Throughput moving ranking for 1536-byte messages on TSMC 65nm.

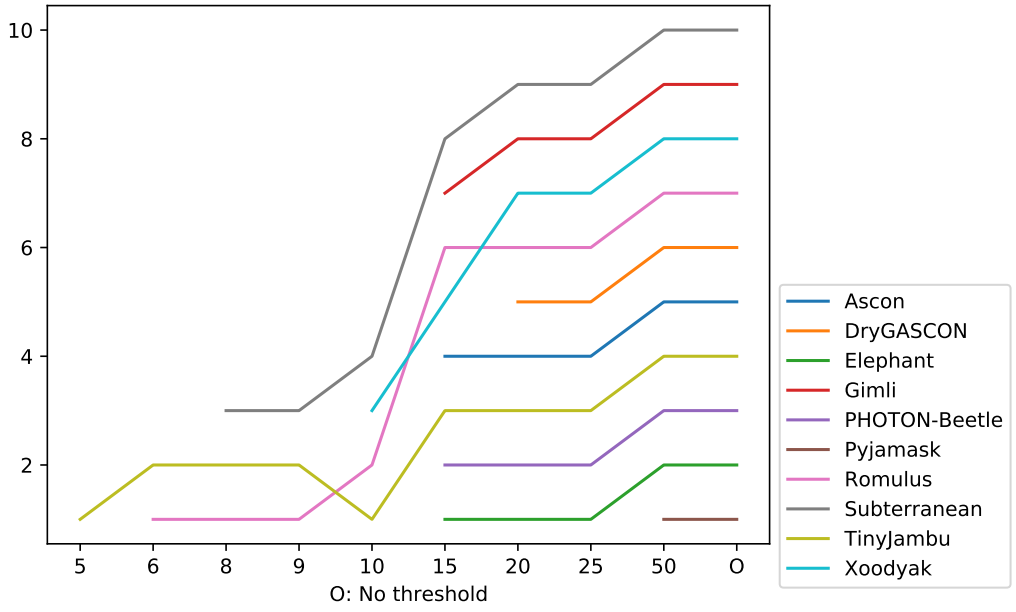

Figure 33: Throughput moving ranking for 1536-byte messages on FDSOI 28nm.

Table 4: Raw synthesis results using the TSMC 65nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
ascon-rp-cg	BC	15490.08	10757.00	0.87	0.56
ascon-rp-cg	LA	15477.12	10748.00	0.84	0.56
ascon-rp-cg	HS	16426.08	11407.00	0.49	6.17
ascon-rp-cg	LF	15475.32	10746.75	1333.33	0.33
ascon-rp-ncg	BC	15826.32	10990.50	0.73	0.93
ascon-rp-ncg	LA	15825.96	10990.25	0.71	0.93
ascon-rp-ncg	HS	16552.08	11494.50	0.49	18.70
ascon-rp-ncg	LF	15811.56	10980.25	1333.33	0.32
beetle-vl-cg	BC	19028.88	13214.50	0.67	0.67
beetle-vl-cg	LA	19028.88	13214.50	0.67	0.67
beetle-vl-cg	HS	25808.04	17922.25	0.49	8.72
beetle-vl-cg	LF	19039.68	13222.00	1292.93	0.39
beetle-vl-ncg	BC	20172.96	14009.00	0.60	1.16
beetle-vl-ncg	LA	20175.84	14011.00	0.60	1.16
beetle-vl-ncg	HS	26795.16	18607.75	0.49	22.24
beetle-vl-ncg	LF	20169.00	14006.25	1292.93	0.40
drygrascon-eh-cg	BC	22353.48	15523.25	0.48	0.70
drygrascon-eh-cg	LA	22354.20	15523.75	0.48	0.70
drygrascon-eh-cg	HS	24561.00	17056.25	0.49	7.14
drygrascon-eh-cg	LF	22337.64	15512.25	2031.75	0.50
drygrascon-eh-ncg	BC	24174.36	16787.75	0.51	1.60
drygrascon-eh-ncg	LA	24174.36	16787.75	0.51	1.60
drygrascon-eh-ncg	HS	26975.88	18733.25	0.49	32.23
drygrascon-eh-ncg	LF	24161.04	16778.50	2031.75	0.51

Table 5: Raw synthesis results using the TSMC 65nm standard cell library (Continued).

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
elephant-rh-1cg	BC	15129.36	10506.50	0.64	0.62
elephant-rh-1cg	LA	15129.36	10506.50	0.64	0.62
elephant-rh-1cg	HS	15676.56	10886.50	0.49	7.51
elephant-rh-1cg	LF	15115.68	10497.00	606.06	0.31
elephant-rh-1ncg	BC	17437.32	12109.25	0.67	1.14
elephant-rh-1ncg	LA	17437.32	12109.25	0.67	1.14
elephant-rh-1ncg	HS	17437.32	12109.25	0.67	1.14
elephant-rh-1ncg	LF	17434.44	12107.25	606.06	0.35
elephant-rh-5cg	BC	21011.40	14591.25	0.73	0.73
elephant-rh-5cg	LA	21011.40	14591.25	0.73	0.73
elephant-rh-5cg	HS	29669.40	20603.75	0.52	9.10
elephant-rh-5cg	LF	20995.92	14580.50	2807.02	0.41
elephant-rh-5ncg	BC	23290.92	16174.25	0.72	1.22
elephant-rh-5ncg	LA	23290.92	16174.25	0.72	1.22
elephant-rh-5ncg	HS	23290.92	16174.25	0.72	1.22
elephant-rh-5ncg	LF	23278.32	16165.50	2807.02	0.44

Table 6: Raw synthesis results using the TSMC 65nm standard cell library (Continued).

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
gimli-pm-12cg	BC	205526.16	142726.50	0.72	5.40
gimli-pm-12cg	LA	205526.16	142726.50	0.72	5.40
gimli-pm-12cg	HS	205526.16	142726.50	0.72	5.40
gimli-pm-12cg	LF	205510.32	142715.50	21333.33	5.15
gimli-pm-12ncg	BC	207151.92	143855.50	0.75	6.04
gimli-pm-12ncg	LA	207151.92	143855.50	0.75	6.04
gimli-pm-12ncg	HS	207151.92	143855.50	0.75	6.04
gimli-pm-12ncg	LF	207253.44	143926.00	21333.33	5.15
gimli-pm-1cg	BC	17334.36	12037.75	0.75	0.48
gimli-pm-1cg	LA	17334.36	12037.75	0.75	0.48
gimli-pm-1cg	HS	18089.28	12562.00	0.49	4.89
gimli-pm-1cg	LF	17310.96	12021.50	1777.78	0.37
gimli-pm-1ncg	BC	18961.56	13167.75	0.75	1.09
gimli-pm-1ncg	LA	18953.28	13162.00	0.78	1.09
gimli-pm-1ncg	HS	19919.52	13833.00	0.49	27.77
gimli-pm-1ncg	LF	18947.16	13157.75	1777.78	0.37
gimli-pm-2cg	BC	20169.36	14006.50	0.75	0.54
gimli-pm-2cg	LA	20169.36	14006.50	0.75	0.54
gimli-pm-2cg	HS	21922.92	15224.25	0.49	5.16
gimli-pm-2cg	LF	20145.24	13989.75	3555.56	0.42
gimli-pm-2ncg	BC	21829.32	15159.25	0.78	1.16
gimli-pm-2ncg	LA	21829.32	15159.25	0.78	1.16
gimli-pm-2ncg	HS	24374.16	16926.50	0.48	28.25
gimli-pm-2ncg	LF	21836.88	15164.50	3555.56	0.44

Table 7: Raw synthesis results using the TSMC 65nm standard cell library (Continued).

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
gimli-pm-3cg	BC	23945.76	16629.00	0.72	0.64
gimli-pm-3cg	LA	23945.76	16629.00	0.72	0.64
gimli-pm-3cg	HS	23945.76	16629.00	0.72	0.64
gimli-pm-3cg	LF	23926.68	16615.75	5333.33	0.52
gimli-pm-3ncg	BC	25673.76	17829.00	0.78	1.28
gimli-pm-3ncg	LA	25673.76	17829.00	0.78	1.28
gimli-pm-3ncg	HS	25673.76	17829.00	0.78	1.28
gimli-pm-3ncg	LF	25682.04	17834.75	5333.33	0.52
gimli-pm-4cg	BC	25454.88	17677.00	0.72	0.70
gimli-pm-4cg	LA	25454.88	17677.00	0.72	0.70
gimli-pm-4cg	HS	25454.88	17677.00	0.72	0.70
gimli-pm-4cg	LF	25435.08	17663.25	7111.11	0.58
gimli-pm-4ncg	BC	27191.52	18883.00	0.75	1.34
gimli-pm-4ncg	LA	27182.16	18876.50	0.78	1.34
gimli-pm-4ncg	HS	27182.16	18876.50	0.78	1.34
gimli-pm-4ncg	LF	27194.76	18885.25	1777.78	0.58
gimli-pm-6cg	BC	32860.80	22820.00	0.72	0.87
gimli-pm-6cg	LA	32860.80	22820.00	0.72	0.87
gimli-pm-6cg	HS	32860.80	22820.00	0.72	0.87
gimli-pm-6cg	LF	32852.52	22814.25	10666.67	0.74
gimli-pm-6ncg	BC	34596.36	24025.25	0.78	1.51
gimli-pm-6ncg	LA	34596.36	24025.25	0.78	1.51
gimli-pm-6ncg	HS	34596.36	24025.25	0.78	1.51
gimli-pm-6ncg	LF	34609.68	24034.50	10666.67	0.74

Table 8: Raw synthesis results using the TSMC 65nm standard cell library (Continued).

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
gimli-pm-8cg	BC	51884.64	36031.00	0.72	1.37
gimli-pm-8cg	LA	51884.64	36031.00	0.72	1.37
gimli-pm-8cg	HS	51884.64	36031.00	0.72	1.37
gimli-pm-8cg	LF	51876.36	36025.25	14222.22	1.22
gimli-pm-8ncg	BC	53594.28	37218.25	0.78	1.93
gimli-pm-8ncg	LA	53594.28	37218.25	0.78	1.93
gimli-pm-8ncg	HS	53594.28	37218.25	0.78	1.93
gimli-pm-8ncg	LF	53610.12	37229.25	14222.22	1.22
pyjamask-rn-fcg	BC	58637.52	40720.50	0.68	1.52
pyjamask-rn-fcg	LA	58646.88	40727.00	0.59	1.53
pyjamask-rn-fcg	HS	56176.92	39011.75	0.49	6.02
pyjamask-rn-fcg	LF	58513.32	40634.25	162.85	1.31
pyjamask-rn-fncg	BC	74188.80	51520.00	0.68	6.40
pyjamask-rn-fncg	LA	74188.80	51520.00	0.68	6.40
pyjamask-rn-fncg	HS	73295.64	50899.75	0.49	136.43
pyjamask-rn-fncg	LF	74088.36	51450.25	162.85	1.93
pyjamask-rn-pcg	BC	59311.80	41188.75	0.68	1.55
pyjamask-rn-pcg	LA	59311.80	41188.75	0.68	1.55
pyjamask-rn-pcg	HS	62574.48	43454.50	0.49	7.86
pyjamask-rn-pcg	LF	59237.28	41137.00	418.30	1.31
pyjamask-rn-pncg	BC	74506.32	51740.50	0.62	5.98
pyjamask-rn-pncg	LA	74506.32	51740.50	0.62	5.98
pyjamask-rn-pncg	HS	80543.52	55933.00	0.49	138.93
pyjamask-rn-pncg	LF	74460.96	51709.00	418.30	1.67

Table 9: Raw synthesis results using the TSMC 65nm standard cell library (Continued).

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
romulus-mk-1cg	BC	8668.44	6019.75	0.90	0.37
romulus-mk-1cg	LA	8672.76	6022.75	0.86	0.37
romulus-mk-1cg	HS	9079.56	6305.25	0.49	4.17
romulus-mk-1cg	LF	8664.84	6017.25	711.11	0.18
romulus-mk-1ncg	BC	9423.72	6544.25	0.76	0.55
romulus-mk-1ncg	LA	9423.72	6544.25	0.76	0.55
romulus-mk-1ncg	HS	9873.00	6856.25	0.49	11.87
romulus-mk-1ncg	LF	9439.20	6555.00	711.11	0.19
romulus-mk-2cg	BC	10069.20	6992.50	0.97	0.40
romulus-mk-2cg	LA	10069.20	6992.50	0.97	0.40
romulus-mk-2cg	HS	11737.08	8150.75	0.48	4.36
romulus-mk-2cg	LF	10059.48	6985.75	1333.33	0.21
romulus-mk-2ncg	BC	10797.12	7498.00	0.85	0.58
romulus-mk-2ncg	LA	10797.12	7498.00	0.85	0.58
romulus-mk-2ncg	HS	12364.20	8586.25	0.49	12.07
romulus-mk-2ncg	LF	10809.00	7506.25	1333.33	0.22
romulus-mk-4cg	BC	13242.24	9196.00	0.80	0.49
romulus-mk-4cg	LA	13242.24	9196.00	0.80	0.49
romulus-mk-4cg	HS	21625.20	15017.50	0.77	5.34
romulus-mk-4cg	LF	13232.16	9189.00	2370.37	0.29
romulus-mk-4ncg	BC	14333.76	9954.00	0.97	0.68
romulus-mk-4ncg	LA	14333.76	9954.00	0.97	0.68
romulus-mk-4ncg	HS	21622.68	15015.75	0.78	11.77
romulus-mk-4ncg	LF	14329.44	9951.00	2370.37	0.30

Table 10: Raw synthesis results using the TSMC 65nm standard cell library (Continued).

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
romulus-mk-8cg	BC	19823.40	13766.25	0.88	0.66
romulus-mk-8cg	LA	19823.40	13766.25	0.88	0.66
romulus-mk-8cg	HS	36947.16	25657.75	1.44	7.44
romulus-mk-8cg	LF	19817.64	13762.25	3878.79	0.45
romulus-mk-8ncg	BC	20874.96	14496.50	0.85	0.84
romulus-mk-8ncg	LA	20874.96	14496.50	0.85	0.84
romulus-mk-8ncg	HS	37909.08	26325.75	1.44	12.60
romulus-mk-8ncg	LF	20874.60	14496.25	3878.79	0.46
romulus-mk-scg	BC	7073.28	4912.00	0.85	0.21
romulus-mk-scg	LA	7073.28	4912.00	0.85	0.21
romulus-mk-scg	HS	7281.36	5056.50	0.49	1.74
romulus-mk-scg	LF	7067.88	4908.25	32.72	0.17
romulus-mk-sncg	BC	8019.72	5569.25	0.76	0.47
romulus-mk-sncg	LA	8019.72	5569.25	0.76	0.47
romulus-mk-sncg	HS	8501.76	5904.00	0.49	11.66
romulus-mk-sncg	LF	8028.72	5575.50	32.72	0.32
subterranean-pm-cg	BC	9599.76	6666.50	0.52	0.43
subterranean-pm-cg	LA	9599.76	6666.50	0.52	0.43
subterranean-pm-cg	HS	9969.12	6923.00	0.49	7.81
subterranean-pm-cg	LF	9593.64	6662.25	10666.67	0.19
subterranean-pm-ncg	BC	9847.08	6838.25	0.43	0.55
subterranean-pm-ncg	LA	9865.80	6851.25	0.47	0.55
subterranean-pm-ncg	HS	10268.28	7130.75	0.49	13.25
subterranean-pm-ncg	LF	9866.16	6851.50	10666.67	0.21

Table 11: Raw synthesis results using the TSMC 65nm standard cell library (Continued).

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
tinyjambu-sl-128cg	BC	5622.12	3904.25	0.82	0.40
tinyjambu-sl-128cg	LA	5622.12	3904.25	0.82	0.40
tinyjambu-sl-128cg	HS	5585.76	3879.00	1.06	1.59
tinyjambu-sl-128cg	LF	5620.32	3903.00	10.40	0.32
tinyjambu-sl-128ncg	BC	6201.36	4306.50	0.58	0.43
tinyjambu-sl-128ncg	LA	6201.36	4306.50	0.58	0.43
tinyjambu-sl-128ncg	HS	6201.36	4306.50	0.77	3.77
tinyjambu-sl-128ncg	LF	6202.44	4307.25	10.40	0.61
tinyjambu-sl-32cg	BC	5695.56	3955.25	0.87	0.40
tinyjambu-sl-32cg	LA	5695.56	3955.25	0.87	0.40
tinyjambu-sl-32cg	HS	5659.20	3930.00	1.17	1.60
tinyjambu-sl-32cg	LF	5691.60	3952.50	161.62	0.13
tinyjambu-sl-32ncg	BC	6395.76	4441.50	0.60	0.44
tinyjambu-sl-32ncg	LA	6395.76	4441.50	0.60	0.44
tinyjambu-sl-32ncg	HS	6359.76	4416.50	0.90	3.74
tinyjambu-sl-32ncg	LF	6397.56	4442.75	161.62	0.16
tinyjambu-sl-8cg	BC	5622.12	3904.25	0.82	0.40
tinyjambu-sl-8cg	LA	5622.12	3904.25	0.82	0.40
tinyjambu-sl-8cg	HS	5585.76	3879.00	1.06	1.59
tinyjambu-sl-8cg	LF	5620.32	3903.00	313.73	0.12
tinyjambu-sl-8ncg	BC	6201.36	4306.50	0.58	0.43
tinyjambu-sl-8ncg	LA	6201.36	4306.50	0.58	0.43
tinyjambu-sl-8ncg	HS	6201.36	4306.50	0.77	3.77
tinyjambu-sl-8ncg	LF	6203.52	4308.00	313.73	0.14

Table 12: Raw synthesis results using the TSMC 65nm standard cell library (Continued).

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
tinyjambu-th-128cg	BC	6806.52	4726.75	0.64	0.27
tinyjambu-th-128cg	LA	6806.52	4726.75	0.64	0.27
tinyjambu-th-128cg	HS	6800.76	4722.75	0.92	0.82
tinyjambu-th-128cg	LF	6801.48	4723.25	1333.33	0.15
tinyjambu-th-128ncg	BC	7517.16	5220.25	0.63	0.46
tinyjambu-th-128ncg	LA	7517.16	5220.25	0.63	0.46
tinyjambu-th-128ncg	HS	7512.84	5217.25	0.88	3.79
tinyjambu-th-128ncg	LF	7517.88	5220.75	1333.33	0.17
tinyjambu-th-32cg	BC	5336.28	3705.75	0.60	0.25
tinyjambu-th-32cg	LA	5336.28	3705.75	0.60	0.25
tinyjambu-th-32cg	HS	5333.40	3703.75	0.84	0.95
tinyjambu-th-32cg	LF	5333.40	3703.75	323.23	0.12
tinyjambu-th-32ncg	BC	6269.40	4353.75	0.61	0.43
tinyjambu-th-32ncg	LA	6269.40	4353.75	0.61	0.43
tinyjambu-th-32ncg	HS	6266.52	4351.75	0.85	3.74
tinyjambu-th-32ncg	LF	6271.20	4355.00	323.23	0.14
tinyjambu-th-8cg	BC	4442.04	3084.75	0.69	0.29
tinyjambu-th-8cg	LA	4442.04	3084.75	0.69	0.29
tinyjambu-th-8cg	HS	4439.52	3083.00	0.75	1.83
tinyjambu-th-8cg	LF	4439.52	3083.00	82.69	0.12
tinyjambu-th-8ncg	BC	5333.40	3703.75	0.58	0.38
tinyjambu-th-8ncg	LA	5333.40	3703.75	0.58	0.38
tinyjambu-th-8ncg	HS	5329.08	3700.75	1.01	3.49
tinyjambu-th-8ncg	LF	5332.32	3703.00	82.69	0.16

Table 13: Raw synthesis results using the TSMC 65nm standard cell library (Continued).

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
xoodyak-sm-12cg	BC	69779.52	48458.00	0.97	2.09
xoodyak-sm-12cg	LA	69779.52	48458.00	0.97	2.09
xoodyak-sm-12cg	HS	69779.52	48458.00	0.97	2.09
xoodyak-sm-12cg	LF	69815.88	48483.25	6400	1.60
xoodyak-sm-12ncg	BC	70594.92	49024.25	0.93	2.13
xoodyak-sm-12ncg	LA	70594.92	49024.25	0.93	2.13
xoodyak-sm-12ncg	HS	70594.92	49024.25	0.93	2.13
xoodyak-sm-12ncg	LF	70608.60	49033.75	6400	1.60
xoodyak-sm-1cg	BC	12667.32	8796.75	0.88	0.73
xoodyak-sm-1cg	LA	12667.32	8796.75	0.88	0.73
xoodyak-sm-1cg	HS	12889.80	8951.25	0.49	15.22
xoodyak-sm-1cg	LF	12667.32	8796.75	3047.62	0.25
xoodyak-sm-1ncg	BC	13472.28	9355.75	0.92	0.84
xoodyak-sm-1ncg	LA	13472.28	9355.75	0.92	0.84
xoodyak-sm-1ncg	HS	13686.12	9504.25	0.49	17.72
xoodyak-sm-1ncg	LF	13464.36	9350.25	3047.62	0.24
xoodyak-sm-2cg	BC	18910.44	13132.25	0.88	0.88
xoodyak-sm-2cg	LA	18910.44	13132.25	0.88	0.88
xoodyak-sm-2cg	HS	24133.32	16759.25	0.49	16.81
xoodyak-sm-2cg	LF	18910.44	13132.25	4266.67	0.40
xoodyak-sm-2ncg	BC	19722.96	13696.50	0.93	0.99
xoodyak-sm-2ncg	LA	19722.96	13696.50	0.93	0.99
xoodyak-sm-2ncg	HS	25027.56	17380.25	0.49	18.08
xoodyak-sm-2ncg	LF	19714.68	13690.75	4266.67	0.39

Table 14: Raw synthesis results using the TSMC 65nm standard cell library (Continued).

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
xoodyak-sm-3cg	BC	25981.92	18043.00	0.88	1.06
xoodyak-sm-3cg	LA	25981.92	18043.00	0.88	1.06
xoodyak-sm-3cg	HS	26534.88	18427.00	0.98	8.34
xoodyak-sm-3cg	LF	25981.92	18043.00	4923.08	0.57
xoodyak-sm-3ncg	BC	26848.80	18645.00	0.93	1.17
xoodyak-sm-3ncg	LA	26848.80	18645.00	0.93	1.17
xoodyak-sm-3ncg	HS	46926.00	32587.50	0.62	20.22
xoodyak-sm-3ncg	LF	26835.48	18635.75	4923.08	0.57
xoodyak-sm-4cg	BC	30830.76	21410.25	0.88	1.17
xoodyak-sm-4cg	LA	30830.76	21410.25	0.88	1.17
xoodyak-sm-4cg	HS	34282.80	23807.50	0.98	9.68
xoodyak-sm-4cg	LF	30830.76	21410.25	5333.33	0.69
xoodyak-sm-4ncg	BC	31641.48	21973.25	0.93	1.28
xoodyak-sm-4ncg	LA	31641.48	21973.25	0.93	1.28
xoodyak-sm-4ncg	HS	53882.28	37418.25	0.82	21.42
xoodyak-sm-4ncg	LF	31629.24	21964.75	5333.33	0.68
xoodyak-sm-6cg	BC	40633.20	28217.50	0.88	1.41
xoodyak-sm-6cg	LA	40633.20	28217.50	0.88	1.41
xoodyak-sm-6cg	HS	40633.20	28217.50	0.88	1.41
xoodyak-sm-6cg	LF	40633.20	28217.50	5818.18	0.92
xoodyak-sm-6ncg	BC	41433.48	28773.25	0.93	1.52
xoodyak-sm-6ncg	LA	41433.48	28773.25	0.93	1.52
xoodyak-sm-6ncg	HS	77376.96	53734.00	1.15	23.06
xoodyak-sm-6ncg	LF	41428.44	28769.75	5818.18	0.91

Table 15: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
ascon-rp-cg	BC	5279.36	10558.71	1.63	0.27
ascon-rp-cg	LA	5279.36	10558.71	1.63	0.27
ascon-rp-cg	HS	6872.84	13745.68	0.60	1.30
ascon-rp-cg	LF	5263.20	10526.40	1333.33	0.23
ascon-rp-ncg	BC	5319.34	10638.68	1.67	0.30
ascon-rp-ncg	LA	5319.34	10638.68	1.67	0.30
ascon-rp-ncg	HS	7488.76	14977.52	0.59	3.15
ascon-rp-ncg	LF	5317.87	10635.74	1333.33	0.22
beetle-vl-cg	BC	6479.20	12958.41	1.51	0.34
beetle-vl-cg	LA	6479.20	12958.41	1.51	0.34
beetle-vl-cg	HS	9314.48	18628.95	0.99	1.89
beetle-vl-cg	LF	6464.19	12928.38	1292.93	0.29
beetle-vl-ncg	BC	6813.11	13626.22	1.36	0.37
beetle-vl-ncg	LA	6806.75	13613.49	1.36	0.37
beetle-vl-ncg	HS	9328.84	18657.68	0.97	3.82
beetle-vl-ncg	LF	6805.93	13611.86	1292.93	0.29
drygrascon-eh-cg	BC	7635.80	15271.60	1.20	0.37
drygrascon-eh-cg	LA	7635.80	15271.60	1.20	0.37
drygrascon-eh-cg	HS	10565.24	21130.48	0.83	1.71
drygrascon-eh-cg	LF	7588.64	15177.27	2031.75	0.34
drygrascon-eh-ncg	BC	8125.24	16250.48	1.06	0.45
drygrascon-eh-ncg	LA	8208.14	16416.29	1.61	0.46
drygrascon-eh-ncg	HS	12341.02	24682.04	0.81	5.43
drygrascon-eh-ncg	LF	8207.65	16415.31	2031.75	0.35

Table 16: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
elephant-rh-1cg	BC	5060.18	10120.36	1.85	0.26
elephant-rh-1cg	LA	5060.18	10120.36	1.85	0.26
elephant-rh-1cg	HS	6247.62	12495.24	0.54	1.50
elephant-rh-1cg	LF	5037.49	10074.99	606.06	0.22
elephant-rh-1ncg	BC	6243.71	12487.41	1.84	0.35
elephant-rh-1ncg	LA	6243.71	12487.41	1.84	0.35
elephant-rh-1ncg	HS	7179.00	14358.01	0.68	3.95
elephant-rh-1ncg	LF	6243.71	12487.41	606.06	0.25
elephant-rh-5cg	BC	7027.72	14055.44	1.59	0.35
elephant-rh-5cg	LA	7027.72	14055.44	1.59	0.35
elephant-rh-5cg	HS	9779.76	19559.52	1.08	1.75
elephant-rh-5cg	LF	7005.52	14011.05	2807.02	0.30
elephant-rh-5ncg	BC	8176.32	16352.64	1.76	0.43
elephant-rh-5ncg	LA	8176.32	16352.64	1.76	0.43
elephant-rh-5ncg	HS	10975.85	21951.71	1.08	4.35
elephant-rh-5ncg	LF	8175.67	16351.33	2807.02	0.34

Table 17: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
gimli-pm-12cg	BC	40170.70	80341.40	1.35	1.82
gimli-pm-12cg	LA	40170.70	80341.40	1.35	1.82
gimli-pm-12cg	HS	40170.70	80341.40	1.35	1.82
gimli-pm-12cg	LF	40149.00	80297.99	21333.33	1.76
gimli-pm-12ncg	BC	40580.50	81160.99	1.22	1.89
gimli-pm-12ncg	LA	40580.50	81160.99	1.22	1.89
gimli-pm-12ncg	HS	40580.50	81160.99	1.22	1.89
gimli-pm-12ncg	LF	40631.58	81263.16	21333.33	1.74
gimli-pm-1cg	BC	5879.44	11758.89	1.36	0.28
gimli-pm-1cg	LA	5879.44	11758.89	1.36	0.28
gimli-pm-1cg	HS	7441.10	14882.21	0.78	1.14
gimli-pm-1cg	LF	5860.68	11721.35	1777.78	0.27
gimli-pm-1ncg	BC	6323.18	12646.37	1.22	0.37
gimli-pm-1ncg	LA	6323.18	12646.37	1.22	0.37
gimli-pm-1ncg	HS	7999.57	15999.15	0.78	4.37
gimli-pm-1ncg	LF	6308.01	12616.01	1777.78	0.27
gimli-pm-2cg	BC	6832.04	13664.08	1.35	0.33
gimli-pm-2cg	LA	6832.04	13664.08	1.35	0.33
gimli-pm-2cg	HS	9541.65	19083.30	0.83	1.39
gimli-pm-2cg	LF	6809.85	13619.69	3555.56	0.31
gimli-pm-2ncg	BC	7441.92	14883.84	1.22	0.42
gimli-pm-2ncg	LA	7441.92	14883.84	1.22	0.42
gimli-pm-2ncg	HS	10111.55	20223.09	0.84	4.65
gimli-pm-2ncg	LF	7426.91	14853.81	3555.56	0.31

Table 18: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
gimli-pm-3cg	BC	8309.98	16619.96	1.35	0.37
gimli-pm-3cg	LA	8309.98	16619.96	1.35	0.37
gimli-pm-3cg	HS	8309.98	16619.96	1.35	0.37
gimli-pm-3cg	LF	8287.79	16575.57	5333.33	0.35
gimli-pm-3ncg	BC	8780.65	17561.30	1.26	0.47
gimli-pm-3ncg	LA	8780.65	17561.30	1.26	0.47
gimli-pm-3ncg	HS	8780.65	17561.30	1.26	0.47
gimli-pm-3ncg	LF	8765.80	17531.60	5333.33	0.35
gimli-pm-4cg	BC	8728.26	17456.53	1.36	0.40
gimli-pm-4cg	LA	8728.26	17456.53	1.36	0.40
gimli-pm-4cg	HS	8728.26	17456.53	1.36	0.40
gimli-pm-4cg	LF	8708.03	17416.05	7111.11	0.38
gimli-pm-4ncg	BC	9200.56	18401.13	1.26	0.49
gimli-pm-4ncg	LA	9200.56	18401.13	1.26	0.49
gimli-pm-4ncg	HS	9200.56	18401.13	1.26	0.49
gimli-pm-4ncg	LF	9186.04	18372.08	7111.11	0.38
gimli-pm-6cg	HS	11161.41	22322.82	1.35	0.51
gimli-pm-6cg	LA	11161.41	22322.82	1.35	0.51
gimli-pm-6cg	BC	11161.41	22322.82	1.35	0.51
gimli-pm-6cg	LF	11139.71	22279.41	10666.67	0.48
gimli-pm-6ncg	BC	11632.41	23264.81	1.22	0.60
gimli-pm-6ncg	LA	11632.41	23264.81	1.22	0.60
gimli-pm-6ncg	HS	11632.41	23264.81	1.22	0.60
gimli-pm-6ncg	LF	11617.88	23235.76	10666.67	0.48

Table 19: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
gimli-pm-8cg	BC	13887.67	27775.33	1.35	0.64
gimli-pm-8cg	LA	13887.67	27775.33	1.35	0.64
gimli-pm-8cg	HS	13887.67	27775.33	1.35	0.64
gimli-pm-8cg	LF	13866.13	27732.25	14222.22	0.61
gimli-pm-8ncg	BC	14353.93	28707.86	1.22	0.73
gimli-pm-8ncg	LA	14353.93	28707.86	1.22	0.73
gimli-pm-8ncg	HS	14353.93	28707.86	1.22	0.73
gimli-pm-8ncg	LF	14339.73	28679.46	14222.22	0.61
pyjamask-rn-fcg	BC	20221.62	40443.25	1.83	0.94
pyjamask-rn-fcg	LA	20221.62	40443.25	1.83	0.94
pyjamask-rn-fcg	HS	21008.90	42017.80	0.70	1.68
pyjamask-rn-fcg	LF	20061.69	40123.37	162.85	0.92
pyjamask-rn-fncg	BC	24552.13	49104.27	1.82	1.54
pyjamask-rn-fncg	LA	24552.13	49104.27	1.83	1.54
pyjamask-rn-fncg	HS	28326.46	56652.92	0.73	21.40
pyjamask-rn-fncg	LF	24496.97	48993.95	162.85	1.02
pyjamask-rn-pcg	BC	20448.31	40896.62	1.91	0.95
pyjamask-rn-pcg	LA	20448.31	40896.62	1.91	0.95
pyjamask-rn-pcg	HS	23661.72	47323.43	0.92	2.05
pyjamask-rn-pcg	LF	20289.02	40578.05	418.30	0.91
pyjamask-rn-pncg	BC	24754.67	49509.33	1.93	1.54
pyjamask-rn-pncg	LA	24754.67	49509.33	1.93	1.54
pyjamask-rn-pncg	HS	28640.62	57281.24	0.97	20.92
pyjamask-rn-pncg	LF	24697.22	49394.44	418.30	0.99

Table 20: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
romulus-mk-1cg	BC	2973.01	5946.03	1.89	0.15
romulus-mk-1cg	LA	2971.55	5943.09	1.80	0.15
romulus-mk-1cg	HS	3693.22	7386.43	0.73	0.88
romulus-mk-1cg	LF	2959.47	5918.94	711.11	0.12
romulus-mk-1ncg	BC	3256.82	6513.64	1.94	0.19
romulus-mk-1ncg	LA	3256.82	6513.64	1.94	0.19
romulus-mk-1ncg	HS	4129.45	8258.90	0.69	1.94
romulus-mk-1ncg	LF	3257.47	6514.94	711.11	0.14
romulus-mk-2cg	BC	3473.39	6946.77	1.93	0.17
romulus-mk-2cg	LA	3473.39	6946.77	1.93	0.17
romulus-mk-2cg	HS	4841.49	9682.98	0.86	0.97
romulus-mk-2cg	LF	3464.41	6928.82	1333.33	0.14
romulus-mk-2ncg	BC	3759.48	7518.95	1.97	0.22
romulus-mk-2ncg	LA	3759.48	7518.95	1.97	0.22
romulus-mk-2ncg	HS	5213.10	10426.20	0.87	2.01
romulus-mk-2ncg	LF	3762.74	7525.48	1333.33	0.16
romulus-mk-4cg	BC	4626.07	9252.13	1.88	0.23
romulus-mk-4cg	LA	4626.07	9252.13	1.88	0.23
romulus-mk-4cg	HS	7588.47	15176.95	1.57	1.24
romulus-mk-4cg	LF	4616.11	9232.22	2370.37	0.19
romulus-mk-4ncg	BC	5221.42	10442.84	1.78	0.27
romulus-mk-4ncg	LA	5221.42	10442.84	1.78	0.27
romulus-mk-4ncg	HS	8234.75	16469.49	1.56	2.25
romulus-mk-4ncg	LF	5223.22	10446.43	2370.37	0.21

Table 21: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
romulus-mk-8cg	BC	7020.37	14040.75	1.85	0.34
romulus-mk-8cg	LA	7020.37	14040.75	1.85	0.34
romulus-mk-8cg	HS	13730.51	27461.01	2.93	2.10
romulus-mk-8cg	LF	7007.48	14014.96	3878.79	0.30
romulus-mk-8ncg	BC	7594.68	15189.35	1.97	0.38
romulus-mk-8ncg	LA	7594.68	15189.35	1.97	0.38
romulus-mk-8ncg	HS	14888.25	29776.49	2.91	2.87
romulus-mk-8ncg	LF	7595.49	15190.98	3878.79	0.32
romulus-mk-scg	BC	2531.88	5063.77	1.75	0.12
romulus-mk-scg	LA	2531.88	5063.77	1.75	0.12
romulus-mk-scg	HS	3112.71	6225.43	0.64	0.44
romulus-mk-scg	LF	2527.48	5054.96	32.72	0.11
romulus-mk-sncg	BC	2760.53	5521.06	1.56	0.16
romulus-mk-sncg	LA	2760.53	5521.06	1.56	0.16
romulus-mk-sncg	HS	3700.07	7400.14	0.67	1.90
romulus-mk-sncg	LF	2760.53	5521.06	32.72	0.14
subterranean-pm-cg	BC	3209.33	6418.66	1.13	0.17
subterranean-pm-cg	LA	3209.33	6418.66	1.13	0.17
subterranean-pm-cg	HS	4171.07	8342.13	0.69	1.53
subterranean-pm-cg	LF	3200.52	6401.03	10666.67	0.13
subterranean-pm-ncg	BC	3370.57	6741.14	0.80	0.18
subterranean-pm-ncg	LA	3370.57	6741.14	0.80	0.18
subterranean-pm-ncg	HS	4405.91	8811.82	0.69	2.22
subterranean-pm-ncg	LF	3370.57	6741.14	10666.67	0.13

Table 22: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
tinyjambu-sl-128cg	BC	1913.03	3826.06	1.58	0.14
tinyjambu-sl-128cg	LA	1913.03	3826.06	1.58	0.14
tinyjambu-sl-128cg	HS	2573.01	5146.02	0.51	0.83
tinyjambu-sl-128cg	LF	1905.69	3811.37	10.40	0.12
tinyjambu-sl-128ncg	BC	2047.18	4094.36	1.50	0.13
tinyjambu-sl-128ncg	LA	2047.18	4094.36	1.50	0.13
tinyjambu-sl-128ncg	HS	2855.51	5711.02	0.51	1.64
tinyjambu-sl-128ncg	LF	2047.67	4095.34	10.40	0.16
tinyjambu-sl-32cg	BC	2033.15	4066.29	1.69	0.14
tinyjambu-sl-32cg	LA	2033.15	4066.29	1.69	0.14
tinyjambu-sl-32cg	HS	2483.58	4967.16	0.52	0.80
tinyjambu-sl-32cg	LF	2026.29	4052.58	161.62	0.09
tinyjambu-sl-32ncg	BC	2178.07	4356.13	1.29	0.14
tinyjambu-sl-32ncg	LA	2178.07	4356.13	1.29	0.14
tinyjambu-sl-32ncg	HS	3086.44	6172.88	0.49	1.65
tinyjambu-sl-32ncg	LF	2177.09	4354.18	161.62	0.10
tinyjambu-sl-8cg	BC	1913.03	3826.06	1.58	0.14
tinyjambu-sl-8cg	LA	1913.03	3826.06	1.58	0.14
tinyjambu-sl-8cg	HS	2573.01	5146.02	0.51	0.83
tinyjambu-sl-8cg	LF	1905.69	3811.37	313.73	0.09
tinyjambu-sl-8ncg	BC	2047.02	4094.04	1.47	0.14
tinyjambu-sl-8ncg	LA	2047.18	4094.36	1.50	0.13
tinyjambu-sl-8ncg	HS	2855.51	5711.02	0.51	1.64
tinyjambu-sl-8ncg	LF	2047.83	4095.67	313.73	0.09

Table 23: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
tinyjambu-th-128cg	BC	2371.95	4743.90	1.37	0.13
tinyjambu-th-128cg	LA	2371.95	4743.90	1.37	0.13
tinyjambu-th-128cg	HS	2386.31	4772.62	0.93	0.23
tinyjambu-th-128cg	LF	2364.12	4728.23	1333.33	0.11
tinyjambu-th-128ncg	BC	2544.78	5089.56	1.65	0.15
tinyjambu-th-128ncg	LA	2544.78	5089.56	1.65	0.15
tinyjambu-th-128ncg	HS	2563.06	5126.11	1.34	0.63
tinyjambu-th-128ncg	LF	2544.29	5088.58	1333.33	0.11
tinyjambu-th-32cg	BC	1886.76	3773.51	1.54	0.11
tinyjambu-th-32cg	LA	1883.82	3767.64	1.55	0.11
tinyjambu-th-32cg	HS	1876.31	3752.62	1.07	0.22
tinyjambu-th-32cg	LF	1875.33	3750.66	323.23	0.09
tinyjambu-th-32ncg	BC	2066.44	4132.88	1.27	0.13
tinyjambu-th-32ncg	LA	2066.44	4132.88	1.27	0.13
tinyjambu-th-32ncg	HS	2077.86	4155.72	1.35	0.60
tinyjambu-th-32ncg	LF	2065.95	4131.90	323.23	0.09
tinyjambu-th-8cg	BC	1568.68	3137.36	1.17	0.10
tinyjambu-th-8cg	LA	1568.68	3137.36	1.17	0.10
tinyjambu-th-8cg	HS	1551.87	3103.74	0.94	0.34
tinyjambu-th-8cg	LF	1549.42	3098.84	82.69	0.07
tinyjambu-th-8ncg	BC	1730.90	3461.80	1.23	0.11
tinyjambu-th-8ncg	LA	1730.90	3461.80	1.23	0.11
tinyjambu-th-8ncg	HS	1735.31	3470.61	1.34	0.55
tinyjambu-th-8ncg	LF	1730.57	3461.15	82.69	0.08

Table 24: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
xoodyak-sm-12cg	BC	26988.22	53976.44	1.76	1.32
xoodyak-sm-12cg	LA	26988.22	53976.44	1.76	1.32
xoodyak-sm-12cg	HS	26988.22	53976.44	1.76	1.32
xoodyak-sm-12cg	LF	26982.18	53964.37	6400	1.24
xoodyak-sm-12ncg	BC	27260.60	54521.20	1.78	1.32
xoodyak-sm-12ncg	LA	27260.60	54521.20	1.78	1.32
xoodyak-sm-12ncg	HS	27260.60	54521.20	1.78	1.32
xoodyak-sm-12ncg	LF	27260.60	54521.20	6400	1.24
xoodyak-sm-1cg	BC	4801.18	9602.36	1.76	0.29
xoodyak-sm-1cg	LA	4801.18	9602.36	1.76	0.29
xoodyak-sm-1cg	HS	6062.23	12124.45	0.60	2.47
xoodyak-sm-1cg	LF	4795.14	9590.28	3047.62	0.20
xoodyak-sm-1ncg	BC	5059.85	10119.71	1.78	0.27
xoodyak-sm-1ncg	LA	5059.85	10119.71	1.78	0.27
xoodyak-sm-1ncg	HS	6718.45	13436.91	0.63	2.61
xoodyak-sm-1ncg	LF	5059.85	10119.71	3047.62	0.20
xoodyak-sm-2cg	BC	7886.15	15772.30	1.76	0.42
xoodyak-sm-2cg	LA	7886.15	15772.30	1.76	0.42
xoodyak-sm-2cg	HS	12168.03	24336.06	0.87	3.34
xoodyak-sm-2cg	LF	7880.11	15760.22	4266.67	0.33
xoodyak-sm-2ncg	BC	8136.34	16272.67	1.78	0.40
xoodyak-sm-2ncg	LA	8136.34	16272.67	1.78	0.40
xoodyak-sm-2ncg	HS	12597.08	25194.16	0.87	3.21
xoodyak-sm-2ncg	LF	8136.34	16272.67	4266.67	0.33

Table 25: Raw synthesis results using the FDSOI 28nm standard cell library.

Implementation	**Corner**	**Area** (μm^2)	**Area** (GE)	**Clock Period** (ns)	**Power** (mW)
xoodyak-sm-3cg	BC	11461.86	22923.72	1.76	0.57
xoodyak-sm-3cg	LA	11461.86	22923.72	1.76	0.57
xoodyak-sm-3cg	HS	15317.30	30634.60	0.93	1.81
xoodyak-sm-3cg	LF	11455.82	22911.65	4923.08	0.48
xoodyak-sm-3ncg	BC	11947.87	23895.74	1.78	0.55
xoodyak-sm-3ncg	LA	11947.87	23895.74	1.78	0.55
xoodyak-sm-3ncg	HS	21387.36	42774.72	1.21	2.93
xoodyak-sm-3ncg	LF	11947.87	23895.74	4923.08	0.49
xoodyak-sm-4cg	BC	14574.25	29148.50	1.76	0.71
xoodyak-sm-4cg	LA	14574.25	29148.50	1.76	0.71
xoodyak-sm-4cg	HS	24825.33	49650.66	1.62	2.95
xoodyak-sm-4cg	LF	14568.21	29136.42	5333.33	0.62
xoodyak-sm-4ncg	BC	14835.21	29670.41	1.78	0.69
xoodyak-sm-4ncg	LA	14835.21	29670.41	1.78	0.69
xoodyak-sm-4ncg	HS	26785.53	53571.05	1.63	3.41
xoodyak-sm-4ncg	LF	14835.21	29670.41	5333.33	0.62
xoodyak-sm-6cg	BC	20050.92	40101.83	1.76	0.97
xoodyak-sm-6cg	LA	20050.92	40101.83	1.76	0.97
xoodyak-sm-6cg	HS	20050.92	40101.83	1.76	0.97
xoodyak-sm-6cg	LF	20048.79	40097.59	5818.18	0.89
xoodyak-sm-6ncg	BC	20315.63	40631.25	1.86	0.95
xoodyak-sm-6ncg	LA	20315.63	40631.25	1.86	0.95
xoodyak-sm-6ncg	HS	36983.24	73966.48	2.37	3.55
xoodyak-sm-6ncg	LF	20315.63	40631.25	5818.18	0.88

Table 26: Minimum energy×area for 16-byte messages on TSMC 65nm.

Candidate	Implementation	Corner	Energy×Area of Auth. (fJ.kGE)	Energy×Area without AD (fJ.kGE)	Energy×Area with AD (fJ.kGE)	AD Cost
TinyJAMBU	tinyjambu-th-128cg	BC	0.0441	0.0610	0.0698	0.1447
Subterranean	subterranean-pm-cg	BC	0.0764	0.0779	0.0823	0.0577
Romulus	romulus-mk-4cg	BC	0.2022	0.2022	0.2022	0
Ascon	ascon-rp-cg	LA	0.3592	0.3288	0.4401	0.3385
Xoodyak	xoodyak-sm-1cg	BC	0.4533	0.4590	0.4760	0.0370
DryGASCON	drygrascon-eh-cg	BC	0.3748	0.3748	0.4842	0.2917
Gimli	gimli-pm-2cg	BC	0.5273	0.5273	0.5953	0.1290
PHOTON-Beetle	beetle-vl-cg	BC	0.4591	0.4770	0.6558	0.3750
Elephant	elephant-rh-5ncg	BC	1.6929	1.3515	1.6929	0.2526
Pyjamask	pyjamask-rn-pcg	BC	25.4045	25.2314	29.8622	0.1835

Table 27: Minimum energy×area for 16-byte messages on FDSOI 28nm.

Candidate	Implementation	Corner	Energy×Area of Auth. (fJ.kGE)	Energy×Area without AD (fJ.kGE)	Energy×Area with AD (fJ.kGE)	AD Cost
Subterranean	subterranean-pm-ncg	BC	0.0508	0.0518	0.0548	0.0577
TinyJAMBU	tinyjambu-th-128cg	BC	0.0481	0.0665	0.0762	0.1447
Romulus	romulus-mk-2cg	BC	0.1958	0.1958	0.1958	0
Ascon	ascon-rp-cg	BC	0.3253	0.2978	0.3986	0.3385
Xoodyak	xoodyak-sm-1ncg	BC	0.3862	0.3910	0.4055	0.0370
DryGASCON	drygrascon-eh-cg	BC	0.4873	0.4873	0.6294	0.2917
Gimli	gimli-pm-2cg	BC	0.5584	0.5584	0.6305	0.1290
PHOTON-Beetle	beetle-vl-cg	BC	0.5190	0.5393	0.7415	0.3750
Elephant	elephant-rh-5cg	BC	0.9196	0.7342	0.9196	0.2526
Pyjamask	pyjamask-rn-pcg	BC	43.3898	43.0941	51.0033	0.1835

Table 28: Minimum energy×area for 64-byte messages on TSMC 65nm.

Candidate	Implementation	Corner	Energy×Area of Auth. (fJ.kGE)	Energy×Area without AD (fJ.kGE)	Energy×Area with AD (fJ.kGE)	AD Cost
Subterranean	subterranean-pm-cg	BC	0.0943	0.0958	0.1183	0.2344
TinyJAMBU	tinyjambu-th-128cg	BC	0.0730	0.1348	0.1758	0.3036
Romulus	romulus-mk-4cg	BC	0.3610	0.3971	0.5559	0.4000
Xoodyak	xoodyak-sm-1cg	BC	0.6063	0.6970	0.8670	0.2439
Ascon	ascon-rp-cg	LA	0.6020	0.5716	0.9257	0.6195
Gimli	gimli-pm-2cg	BC	0.7314	0.7314	1.0035	0.3721
DryGASCON	drygrascon-eh-cg	BC	0.7028	0.7028	1.1401	0.6222
PHOTON-Beetle	beetle-vl-cg	BC	0.9599	1.0672	1.7469	0.6369
Elephant	elephant-rh-5cg	BC	1.2932	1.7346	2.2921	0.3214
Pyjamask	pyjamask-rn-pcg	BC	38.1284	38.4746	55.8293	0.4511

Table 29: Minimum energy×area for 64-byte messages on FDSOI 28nm.

Candidate	Implementation	Corner	Energy×Area of Auth. (fJ.kGE)	Energy×Area without AD (fJ.kGE)	Energy×Area with AD (fJ.kGE)	AD Cost
Subterranean	subterranean-pm-ncg	BC	0.0628	0.0637	0.0787	0.2344
TinyJAMBU	tinyjambu-th-128cg	BC	0.0797	0.1471	0.1917	0.3036
Romulus	romulus-mk-2cg	BC	0.3637	0.4197	0.5875	0.4000
Xoodyak	xoodyak-sm-1ncg	BC	0.5165	0.5938	0.7386	0.2439
Ascon	ascon-rp-cg	BC	0.5452	0.5177	0.8384	0.6195
Gimli	gimli-pm-2cg	BC	0.7746	0.7746	1.0628	0.3721
DryGASCON	drygrascon-eh-cg	BC	0.9136	0.9136	1.4821	0.6222
PHOTON-Beetle	beetle-vl-cg	BC	1.0853	1.2066	1.9751	0.6369
Elephant	elephant-rh-5cg	BC	1.2906	1.7311	2.2875	0.3214
Pyjamask	pyjamask-rn-pcg	BC	65.1217	65.7130	95.3541	0.4511

Table 30: Minimum energy×area for 1536-byte messages on TSMC 65nm.

Candidate	Implementation	Corner	Energy×Area of Auth. (fJ.kGE)	Energy×Area without AD (fJ.kGE)	Energy×Area with AD (fJ.kGE)	AD Cost
Subterranean	subterranean-pm-cg	BC	0.6453	0.6468	1.2202	0.8866
TinyJAMBU	tinyjambu-th-128cg	BC	0.9591	2.5008	3.4245	0.3694
Romulus	romulus-mk-4cg	BC	4.0143	6.3752	10.1874	0.5980
Gimli	gimli-pm-3cg	BC	6.3952	6.3876	12.2562	0.9188
Xoodyak	xoodyak-sm-1cg	BC	5.4965	7.9671	13.0273	0.6351
Ascon	ascon-rp-cg	LA	8.0482	8.0178	15.8181	0.9729
DryGASCON	drygrascon-eh-cg	BC	10.7611	10.7611	21.2566	0.9753
PHOTON-Beetle	beetle-vl-cg	BC	16.3182	19.1681	35.2062	0.8367
Elephant	elephant-rh-5cg	BC	15.0461	26.0421	40.3525	0.5495
Pyjamask	pyjamask-rn-pcg	BC	428.3273	444.6001	852.1537	0.9167

Table 31: Minimum energy×area for 1536-byte messages on FDSOI 28nm.

Candidate	Implementation	Corner	Energy×Area of Auth. (fJ.kGE)	Energy×Area without AD (fJ.kGE)	Energy×Area with AD (fJ.kGE)	AD Cost
Subterranean	subterranean-pm-ncg	BC	0.4293	0.4303	0.8118	0.8866
TinyJAMBU	tinyjambu-th-128cg	BC	1.0461	2.7279	3.7355	0.3694
Romulus	romulus-mk-4cg	BC	4.3694	6.9392	11.0885	0.5980
Xoodyak	xoodyak-sm-1ncg	BC	4.6827	6.7875	11.0984	0.6351
Gimli	gimli-pm-3cg	BC	7.0113	7.0030	13.4370	0.9188
Ascon	ascon-rp-cg	BC	7.2891	7.2617	14.3263	0.9729
DryGASCON	drygrascon-eh-cg	BC	13.9890	13.9890	27.6328	0.9753
PHOTON-Beetle	beetle-vl-cg	BC	18.4498	21.6720	39.8050	0.8367
Elephant	elephant-rh-5cg	BC	15.0155	25.9892	40.2705	0.5495
Pyjamask	pyjamask-rn-pcg	BC	731.5654	759.3585	1455.4433	0.9167

Table 32: Minimum energy for 16-byte messages on TSMC 65nm.

Candidate	Implementation	Corner	Energy of Auth. (pJ)	Energy without AD (pJ)	Energy with AD (pJ)	AD Cost
Subterranean	subterranean-pm-cg	BC	11.45	11.68	12.35	0.0577
TinyJAMBU	tinyjambu-th-128cg	BC	9.34	12.90	14.77	0.1447
Romulus	romulus-mk-4cg	BC	21.98	21.98	21.98	0
DryGASCON	drygrascon-eh-cg	BC	24.15	24.15	31.19	0.2917
Gimli	gimli-pm-3cg	BC	35.80	35.34	39.47	0.1169
Ascon	ascon-rp-cg	LA	33.42	30.59	40.95	0.3385
Xoodyak	xoodyak-sm-2cg	BC	43.42	44.20	46.52	0.0526
PHOTON-Beetle	beetle-vl-cg	BC	34.74	36.09	49.63	0.3750
Elephant	elephant-rh-5cg	BC	63.15	50.42	63.15	0.2526
Pyjamask	pyjamask-rn-pcg	BC	616.78	612.58	725.01	0.1835

Table 33: Minimum energy for 16-byte messages on FDSOI 28nm.

Candidate	Implementation	Corner	Energy of Auth. (pJ)	Energy without AD (pJ)	Energy with AD (pJ)	AD Cost
Subterranean	subterranean-pm-ncg	BC	7.54	7.68	8.13	0.0577
TinyJAMBU	tinyjambu-th-128cg	BC	10.15	14.02	16.05	0.1447
Romulus	romulus-mk-4cg	BC	23.78	23.78	23.78	0
Ascon	ascon-rp-cg	BC	30.81	28.20	37.75	0.3385
Xoodyak	xoodyak-sm-1ncg	BC	38.16	38.64	40.07	0.0370
DryGASCON	drygrascon-eh-cg	BC	31.91	31.91	41.21	0.2917
Gimli	gimli-pm-4cg	BC	39.28	38.73	43.09	0.1127
PHOTON-Beetle	beetle-vl-ncg	BC	38.67	40.18	55.25	0.3750
Elephant	elephant-rh-5cg	BC	65.43	52.23	65.43	0.2526
Pyjamask	pyjamask-rn-pcg	BC	1060.96	1053.73	1247.13	0.1835

Table 34: Minimum energy for 64-byte messages on TSMC 65nm.

Candidate	Implementation	Corner	Energy of Auth. (pJ)	Energy without AD (pJ)	Energy with AD (pJ)	AD Cost
Subterranean	subterranean-pm-cg	BC	14.15	14.37	17.74	0.2344
TinyJAMBU	tinyjambu-th-128cg	BC	15.45	28.53	37.18	0.3036
Romulus	romulus-mk-4cg	BC	39.26	43.18	60.45	0.4000
Gimli	gimli-pm-3cg	BC	46.81	46.35	61.50	0.3267
DryGASCON	drygrascon-eh-cg	BC	45.28	45.28	73.45	0.6222
Xoodyak	xoodyak-sm-2cg	BC	59.70	67.46	86.07	0.2759
Ascon	ascon-rp-cg	LA	56.01	53.18	86.13	0.6195
PHOTON-Beetle	beetle-vl-cg	BC	72.64	80.76	132.20	0.6369
Elephant	elephant-rh-5cg	BC	88.63	118.88	157.09	0.3214
Pyjamask	pyjamask-rn-pcg	BC	925.70	934.10	1355.45	0.4511

Table 35: Minimum energy for 64-byte messages on FDSOI 28nm.

Candidate	Implementation	Corner	Energy of Auth. (pJ)	Energy without AD (pJ)	Energy with AD (pJ)	AD Cost
Subterranean	subterranean-pm-cg	BC	14.15	14.37	17.74	0.2344
TinyJAMBU	tinyjambu-th-128cg	BC	15.45	28.53	37.18	0.3036
Romulus	romulus-mk-4cg	BC	39.26	43.18	60.45	0.4000
Gimli	gimli-pm-3cg	BC	46.81	46.35	61.50	0.3267
DryGASCON	drygrascon-eh-cg	BC	45.28	45.28	73.45	0.6222
Xoodyak	xoodyak-sm-2cg	BC	59.70	67.46	86.07	0.2759
Ascon	ascon-rp-cg	LA	56.01	53.18	86.13	0.6195
PHOTON-Beetle	beetle-vl-cg	BC	72.64	80.76	132.20	0.6369
Elephant	elephant-rh-5cg	BC	88.63	118.88	157.09	0.3214
Pyjamask	pyjamask-rn-pcg	BC	925.70	934.10	1355.45	0.4511

Table 36: Minimum energy for 1536-byte messages on TSMC 65nm.

Candidate	Implementation	Corner	Energy of Auth. (pJ)	Energy without AD (pJ)	Energy with AD (pJ)	AD Cost
Subterranean	subterranean-pm-cg	BC	96.80	97.02	183.04	0.8866
TinyJAMBU	tinyjambu-th-128cg	BC	202.90	529.07	724.50	0.3694
Gimli	gimli-pm-3cg	BC	384.58	384.12	737.04	0.9188
Romulus	romulus-mk-8cg	BC	443.98	633.34	1052.84	0.6624
Xoodyak	xoodyak-sm-2cg	BC	575.32	778.47	1312.70	0.6863
DryGASCON	drygrascon-eh-cg	BC	693.22	693.22	1369.34	0.9753
Ascon	ascon-rp-cg	LA	748.81	745.98	1471.73	0.9729
PHOTON-Beetle	beetle-vl-cg	BC	1234.87	1450.54	2664.21	0.8367
Elephant	elephant-rh-5ncg	BC	1708.97	2957.93	4583.35	0.5495
Pyjamask	pyjamask-rn-pcg	BC	10399.13	10794.21	20688.99	0.9167

Table 37: Minimum energy for 1536-byte messages on FDSOI 28nm.

Candidate	Implementation	Corner	Energy of Auth. (pJ)	Energy without AD (pJ)	Energy with AD (pJ)	AD Cost
Subterranean	subterranean-pm-ncg	BC	63.68	63.83	120.42	0.8866
TinyJAMBU	tinyjambu-th-128cg	BC	220.52	575.02	787.43	0.3694
Gimli	gimli-pm-3cg	BC	421.86	421.36	808.48	0.9188
Xoodyak	xoodyak-sm-1ncg	BC	462.73	670.72	1096.71	0.6351
Romulus	romulus-mk-8cg	BC	479.44	683.92	1136.94	0.6624
Ascon	ascon-rp-cg	BC	690.34	687.74	1356.82	0.9729
DryGASCON	drygrascon-eh-cg	BC	916.01	916.01	1809.42	0.9753
Elephant	elephant-rh-5cg	BC	1068.30	1849.05	2865.12	0.5495
PHOTON-Beetle	beetle-vl-ncg	BC	1374.65	1614.73	2965.77	0.8367
Pyjamask	pyjamask-rn-pcg	BC	17888.16	18567.76	35588.36	0.9167

Table 38: Maximum throughput for 16-byte messages on TSMC 65nm.

Candidate	Implementation	Corner	Throughput of Auth. (Gbps)	Throughput without AD (Gbps)	Throughput with AD (Gbps)	AD Efficiency
Subterranean	subterranean-pm-ncg	BC	5.84	5.72	10.82	0.8909
Romulus	romulus-mk-8ncg	BC	3.59	3.59	7.17	1
Xoodyak	xoodyak-sm-12ncg	BC	3.82	3.72	6.88	0.8500
DryGASCON	drygrascon-eh-cg	BC	3.70	3.70	5.73	0.5484
Gimli	gimli-pm-8cg	BC	2.69	2.58	4.80	0.8649
TinyJAMBU	tinyjambu-th-128ncg	BC	3.69	2.67	4.67	0.7471
Ascon	ascon-rp-ncg	LA	2.54	2.77	4.14	0.4943
PHOTON-Beetle	beetle-vl-ncg	BC	2.77	2.67	3.88	0.4545
Elephant	elephant-rh-5ncg	BC	1.49	1.87	2.99	0.5966
Pyjamask	pyjamask-rn-pncg	BC	0.35	0.35	0.60	0.6899

Table 39: Maximum throughput for 16-byte messages on FDSOI 28nm.

Candidate	Implementation	Corner	Throughput of Auth. (Gbps)	Throughput without AD (Gbps)	Throughput with AD (Gbps)	AD Efficiency
Subterranean	subterranean-pm-ncg	BC	3.14	3.08	5.82	0.8909
Xoodyak	xoodyak-sm-12cg	BC	2.02	1.97	3.64	0.8500
Romulus	romulus-mk-8cg	BC	1.65	1.65	3.29	1
Gimli	gimli-pm-8ncg	BC	1.59	1.52	2.84	0.8649
DryGASCON	drygrascon-eh-ncg	BC	1.68	1.68	2.60	0.5484
TinyJAMBU	tinyjambu-th-128cg	BC	1.70	1.23	2.15	0.7471
Ascon	ascon-rp-cg	BC	1.11	1.21	1.81	0.4943
PHOTON-Beetle	beetle-vl-ncg	BC	1.22	1.18	1.71	0.4545
Elephant	elephant-rh-5cg	BC	0.68	0.85	1.35	0.5966
Pyjamask	pyjamask-rn-pcg	BC	0.11	0.11	0.19	0.6899

Table 40: Maximum throughput for 64-byte messages on TSMC 65nm.

Candidate	Implementation	Corner	Throughput of Auth. (Gbps)	Throughput without AD (Gbps)	Throughput with AD (Gbps)	AD Efficiency
Subterranean	subterranean-pm-ncg	BC	18.90	18.60	30.14	0.6203
Xoodyak	xoodyak-sm-12ncg	BC	10.59	9.66	14.49	0.5000
Gimli	gimli-pm-8cg	BC	7.90	7.65	11.66	0.5246
Romulus	romulus-mk-8ncg	BC	8.37	8.03	11.47	0.4286
DryGASCON	drygrascon-eh-cg	BC	7.90	7.90	9.74	0.2329
Ascon	ascon-rp-ncg	LA	6.06	6.38	7.88	0.2350
TinyJAMBU	tinyjambu-th-128ncg	BC	8.93	4.84	7.42	0.5342
PHOTON-Beetle	beetle-vl-ncg	BC	5.30	4.77	5.82	0.2218
Pyjamask	pyjamask-rn-pncg	BC	0.94	0.93	1.28	0.3783

Table 41: Maximum throughput for 64-byte messages on FDSOI 28nm.

Candidate	Implementation	Corner	Throughput of Auth. (Gbps)	Throughput without AD (Gbps)	Throughput with AD (Gbps)	AD Efficiency
Subterranean	subterranean-pm-ncg	BC	10.16	10	16.20	0.6203
Xoodyak	xoodyak-sm-12cg	BC	5.59	5.10	7.66	0.5000
Gimli	gimli-pm-8ncg	BC	4.66	4.51	6.88	0.5246
Romulus	romulus-mk-8cg	BC	3.84	3.69	5.27	0.4286
DryGASCON	drygrascon-eh-ncg	BC	3.58	3.58	4.41	0.2329
Ascon	ascon-rp-cg	BC	2.64	2.78	3.43	0.2350
PHOTON-Beetle	beetle-vl-ncg	BC	2.34	2.10	2.57	0.2218
Elephant	elephant-rh-5cg	BC	1.93	1.44	2.18	0.5135
Pyjamask	pyjamask-rn-pcg	BC	0.30	0.30	0.42	0.3783

Table 42: Maximum throughput for 1536-byte messages on TSMC 65nm.

Candidate	Implementation	Corner	Throughput of Auth. (Gbps)	Throughput without AD (Gbps)	Throughput with AD (Gbps)	AD Efficiency
Subterranean	subterranean-pm-ncg	BC	66.30	66.15	70.13	0.0601
Xoodyak	xoodyak-sm-12ncg	BC	23.94	19.75	22.24	0.1263
Gimli	gimli-pm-8cg	BC	20.66	20.59	21.41	0.0402
Romulus	romulus-mk-8ncg	BC	18.97	13.30	16.00	0.2031
DryGASCON	drygrascon-eh-cg	BC	12.39	12.39	12.54	0.0125
Ascon	ascon-rp-ncg	LA	10.88	10.92	11.07	0.0138
TinyJAMBU	tinyjambu-th-128ncg	BC	16.32	6.26	9.14	0.4605
PHOTON-Beetle	beetle-vl-ncg	BC	7.48	6.37	6.94	0.0889
Elephant	elephant-rh-5ncg	BC	8.78	5.07	6.55	0.2907
Pyjamask	pyjamask-rn-pncg	BC	2.00	1.93	2.01	0.0435

Table 43: Maximum throughput for 1536-byte messages on FDSOI 28nm.

Candidate	Implementation	Corner	Throughput of Auth. (Gbps)	Throughput without AD (Gbps)	Throughput with AD (Gbps)	AD Efficiency
Subterranean	subterranean-pm-ncg	BC	35.64	35.56	37.69	0.0601
Gimli	gimli-pm-8ncg	BC	12.19	12.15	12.64	0.0402
Xoodyak	xoodyak-sm-12cg	BC	12.65	10.44	11.75	0.1263
Romulus	romulus-mk-8cg	BC	8.72	6.11	7.35	0.2031
DryGASCON	drygrascon-eh-ncg	BC	5.61	5.61	5.68	0.0125
Ascon	ascon-rp-cg	BC	4.74	4.76	4.82	0.0138
TinyJAMBU	tinyjambu-th-128cg	BC	7.51	2.88	4.20	0.4605
PHOTON-Beetle	beetle-vl-ncg	BC	3.30	2.81	3.06	0.0889
Elephant	elephant-rh-5cg	BC	3.98	2.30	2.97	0.2907
Pyjamask	pyjamask-rn-pcg	BC	0.65	0.63	0.65	0.0435

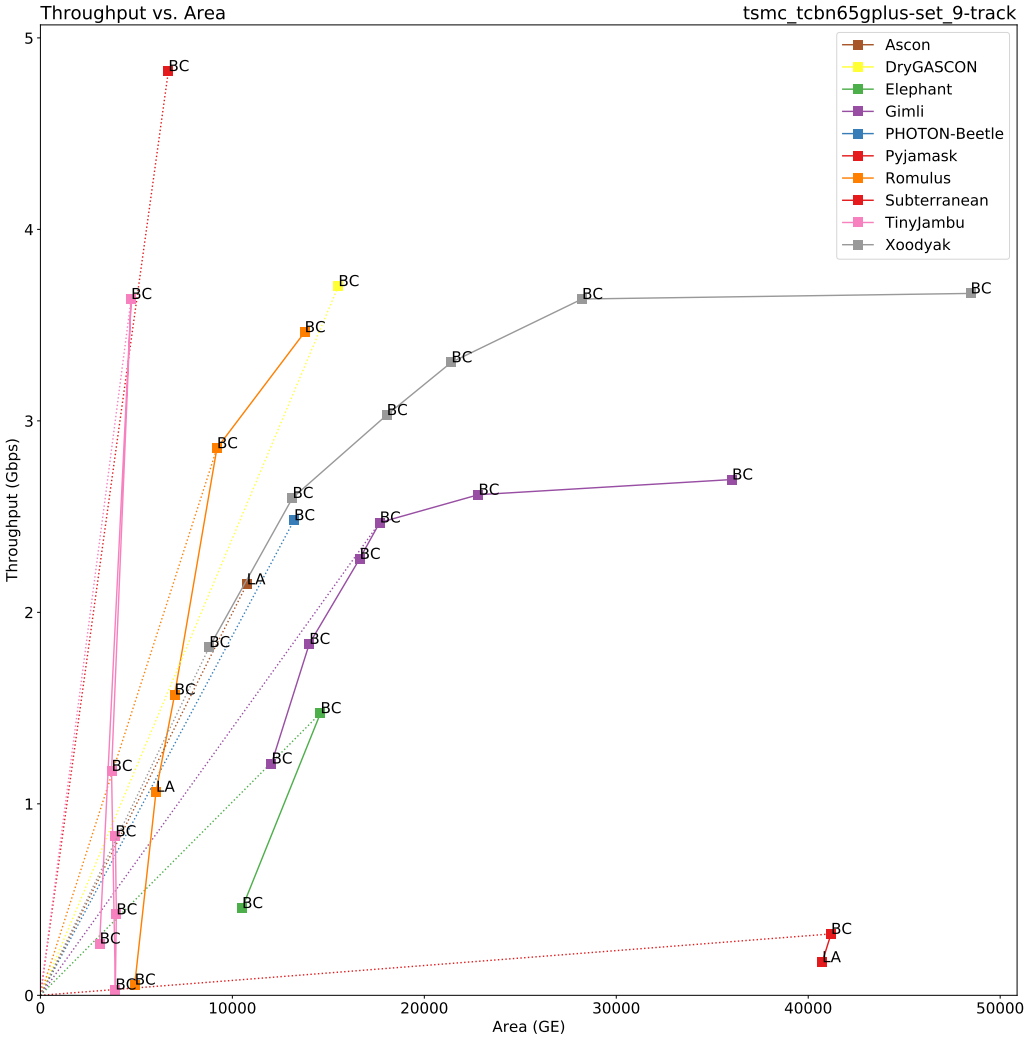

Figure 34: Throughput vs. Area for $|A| = 16$ bytes on TSMC 65nm.

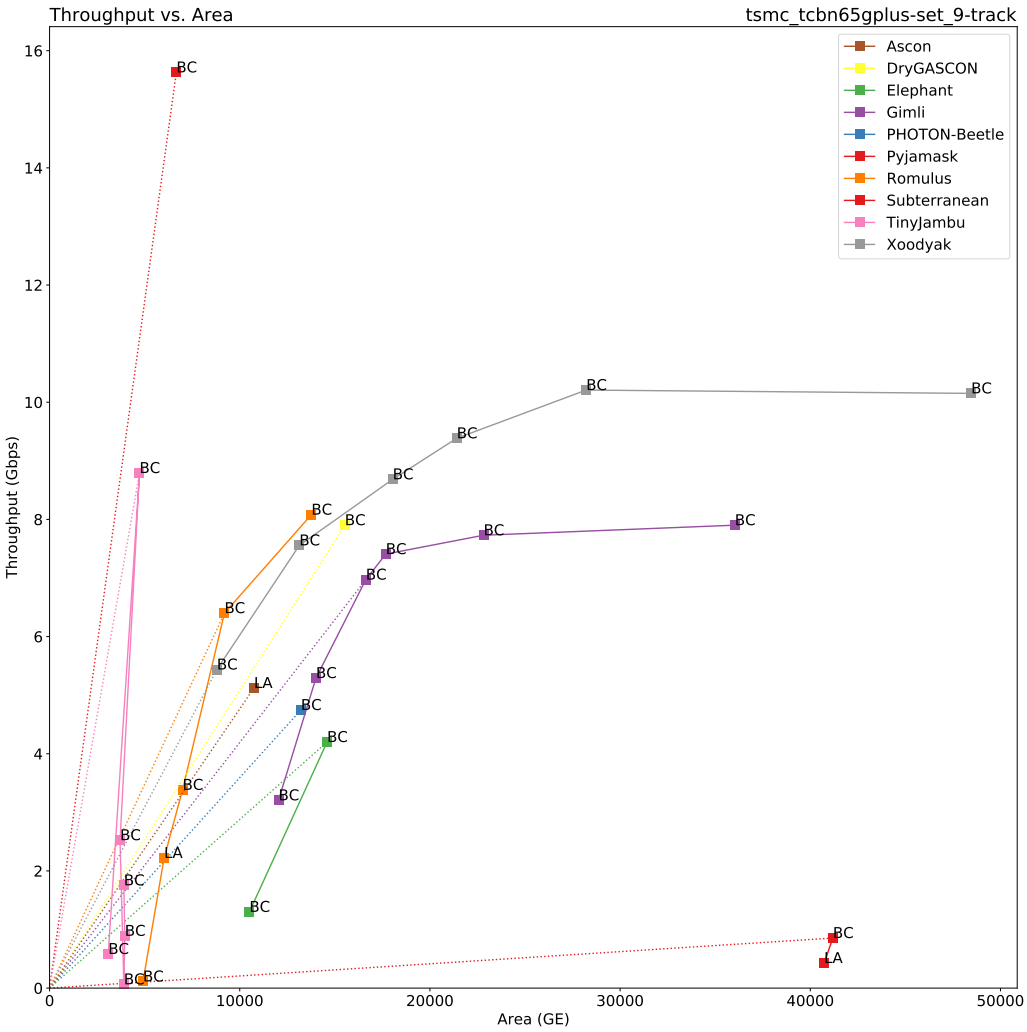

Figure 35: Throughput vs. Area for $|A| = 64$ bytes on TSMC 65nm.

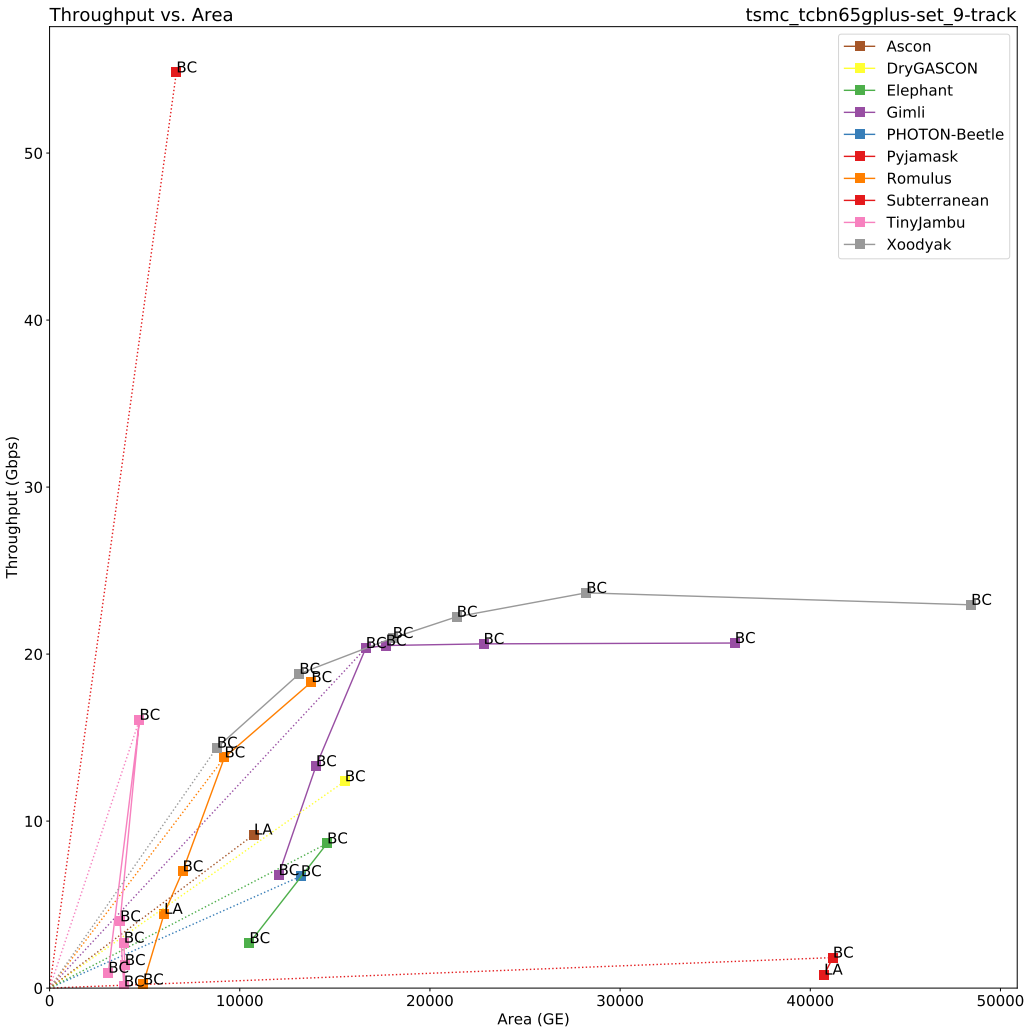

Figure 36: Throughput vs. Area for |A| = 1536 bytes on TSMC 65nm.

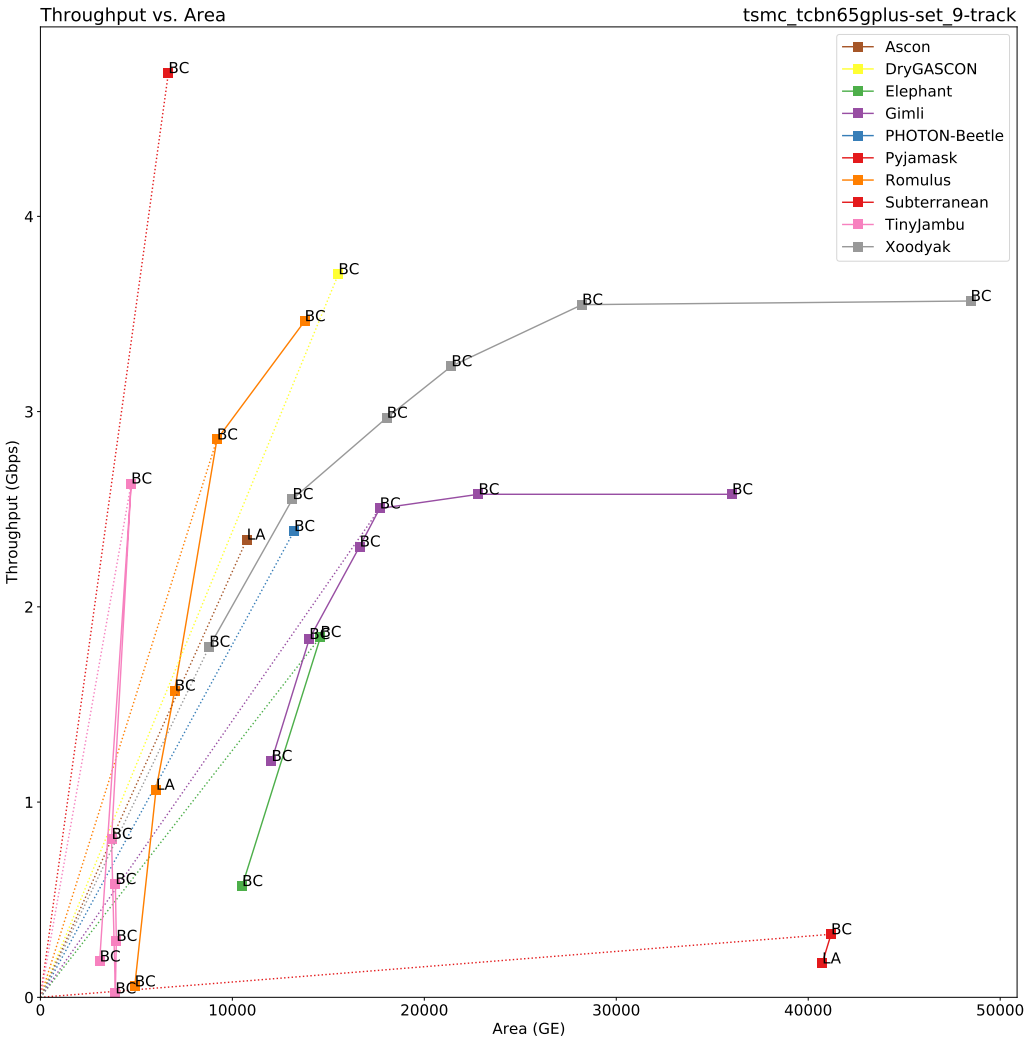

Figure 37: Throughput vs. Area for $|M| = 16$ bytes on TSMC 65nm.

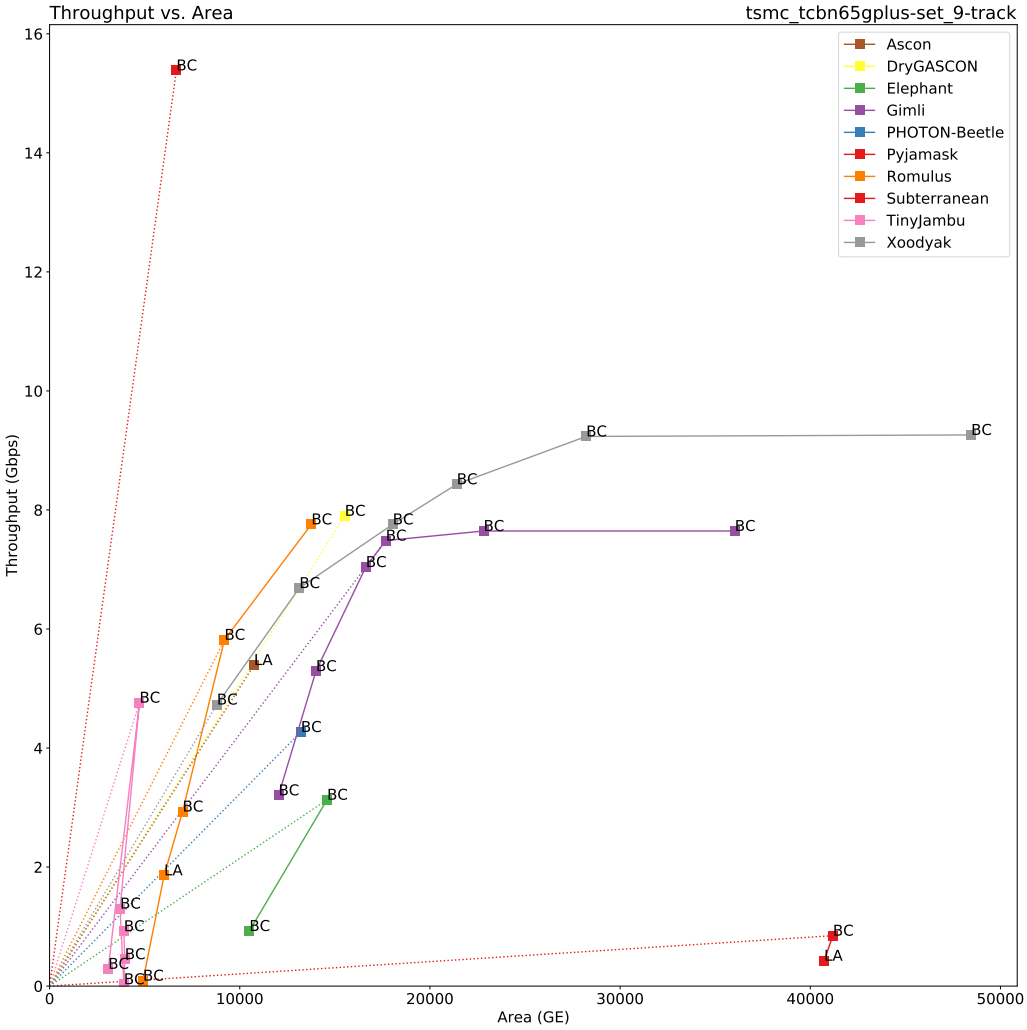

Figure 38: Throughput vs. Area for |M| = 64 bytes on TSMC 65nm.

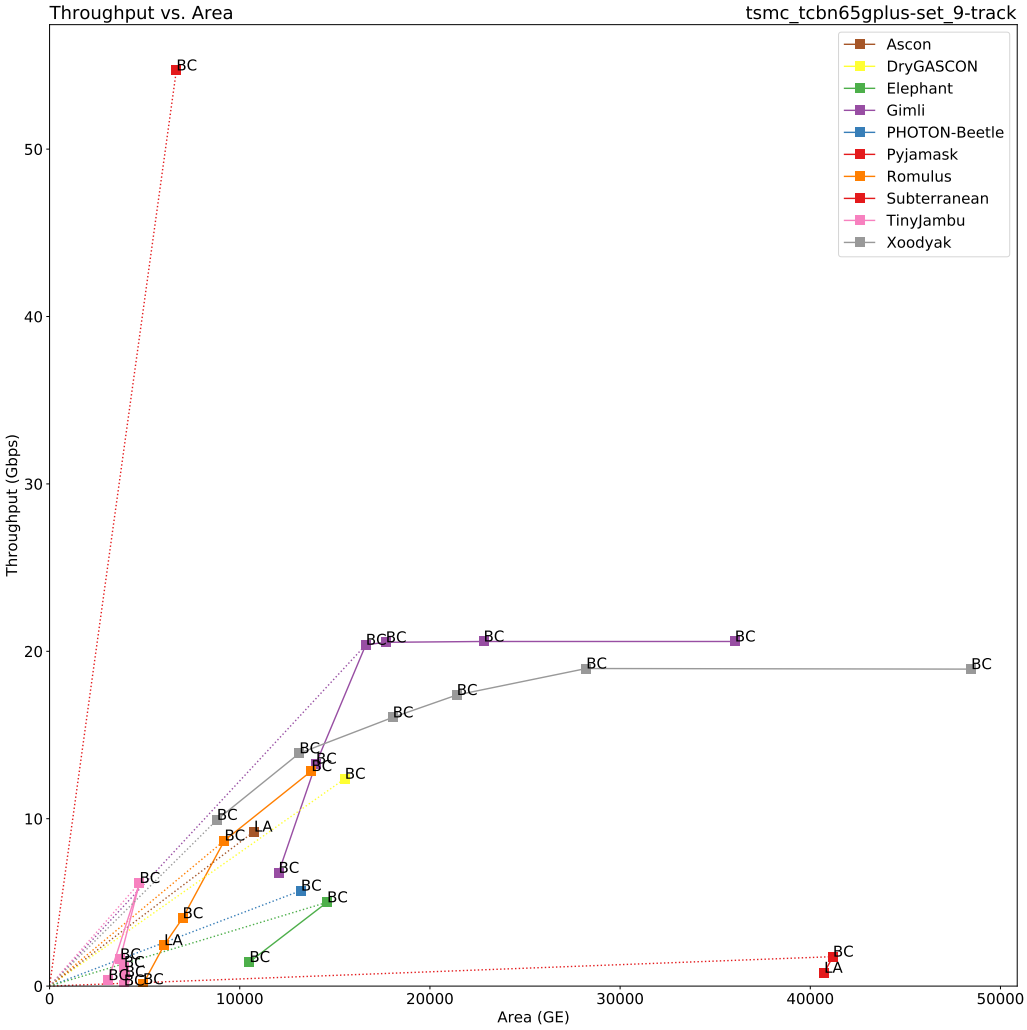

Figure 39: Throughput vs. Area for |M| = 1536 bytes on TSMC 65nm.

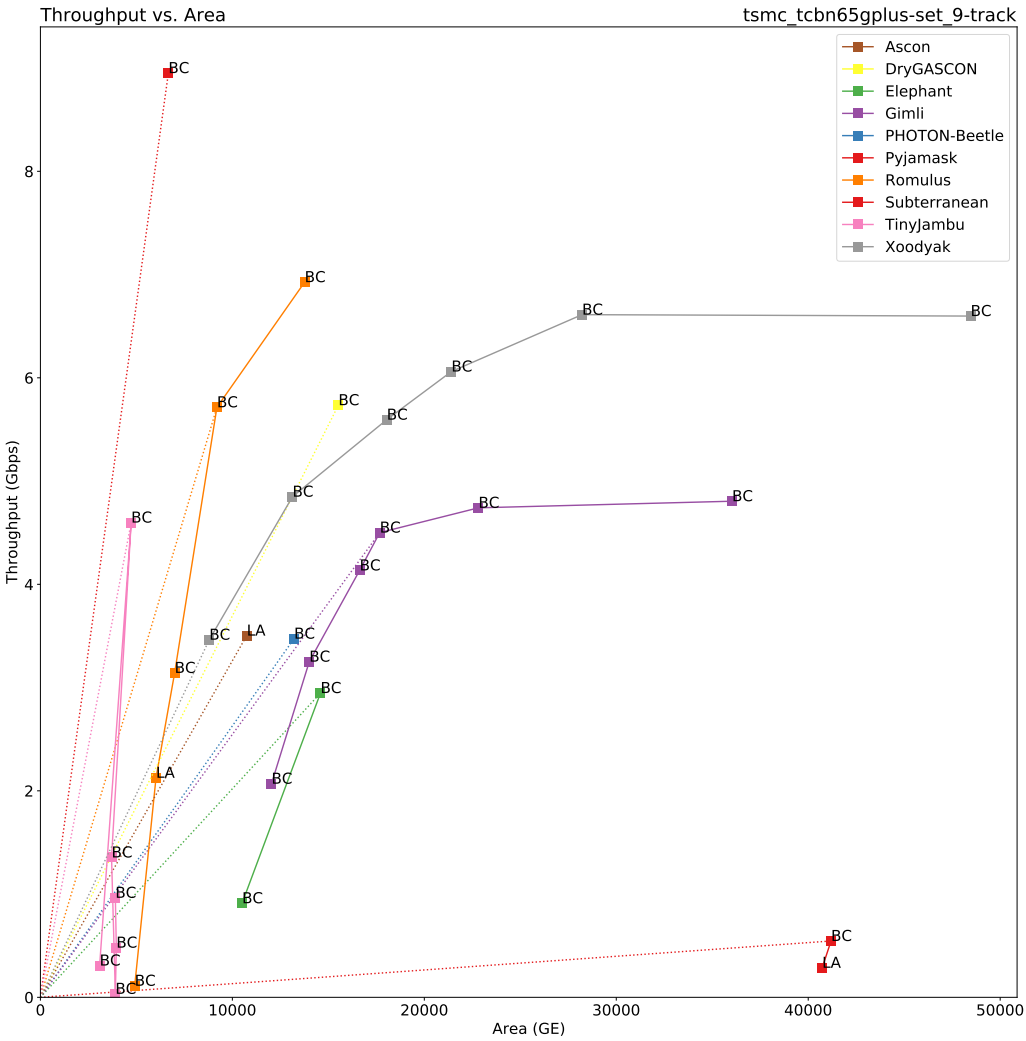

Figure 40: Throughput vs. Area for |A| = |M| = 16 bytes on TSMC 65nm.

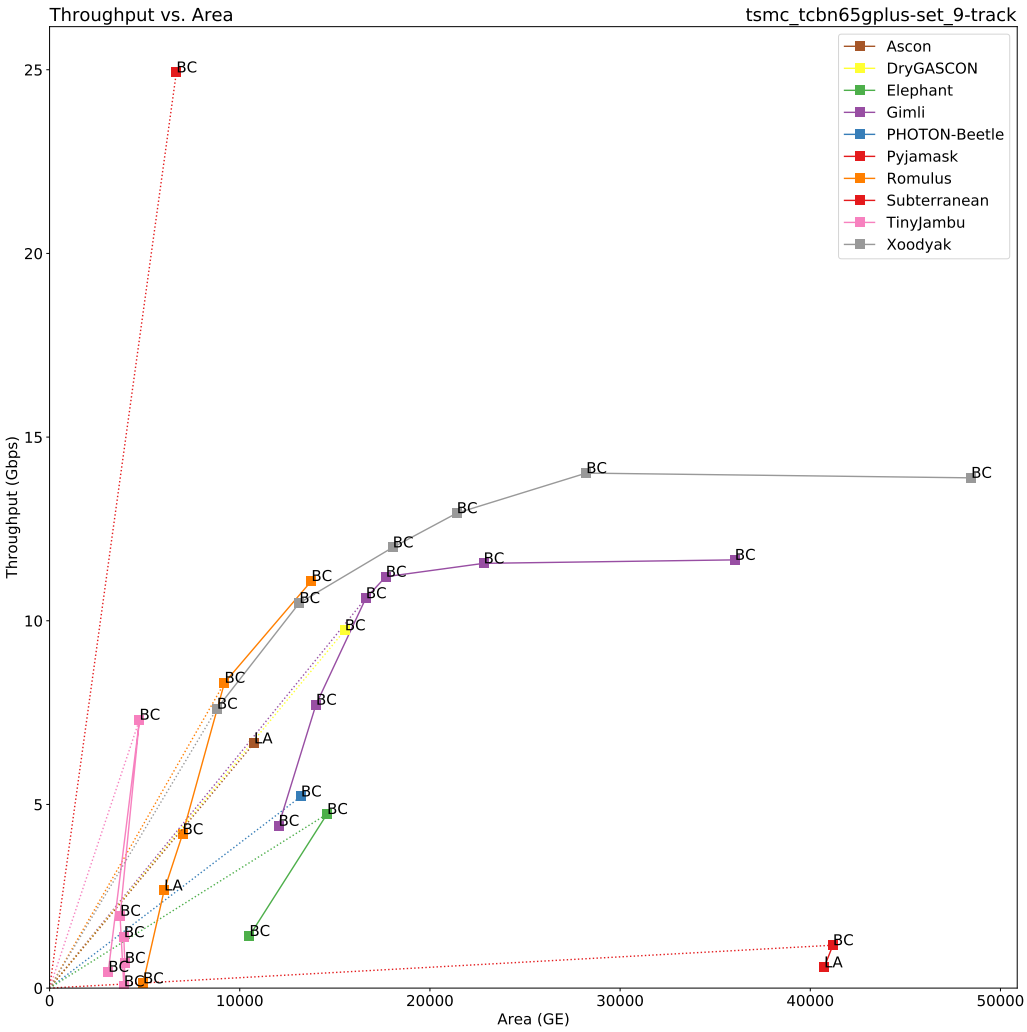

Figure 41: Throughput vs. Area for |A| = |M| = 64 bytes on TSMC 65nm.

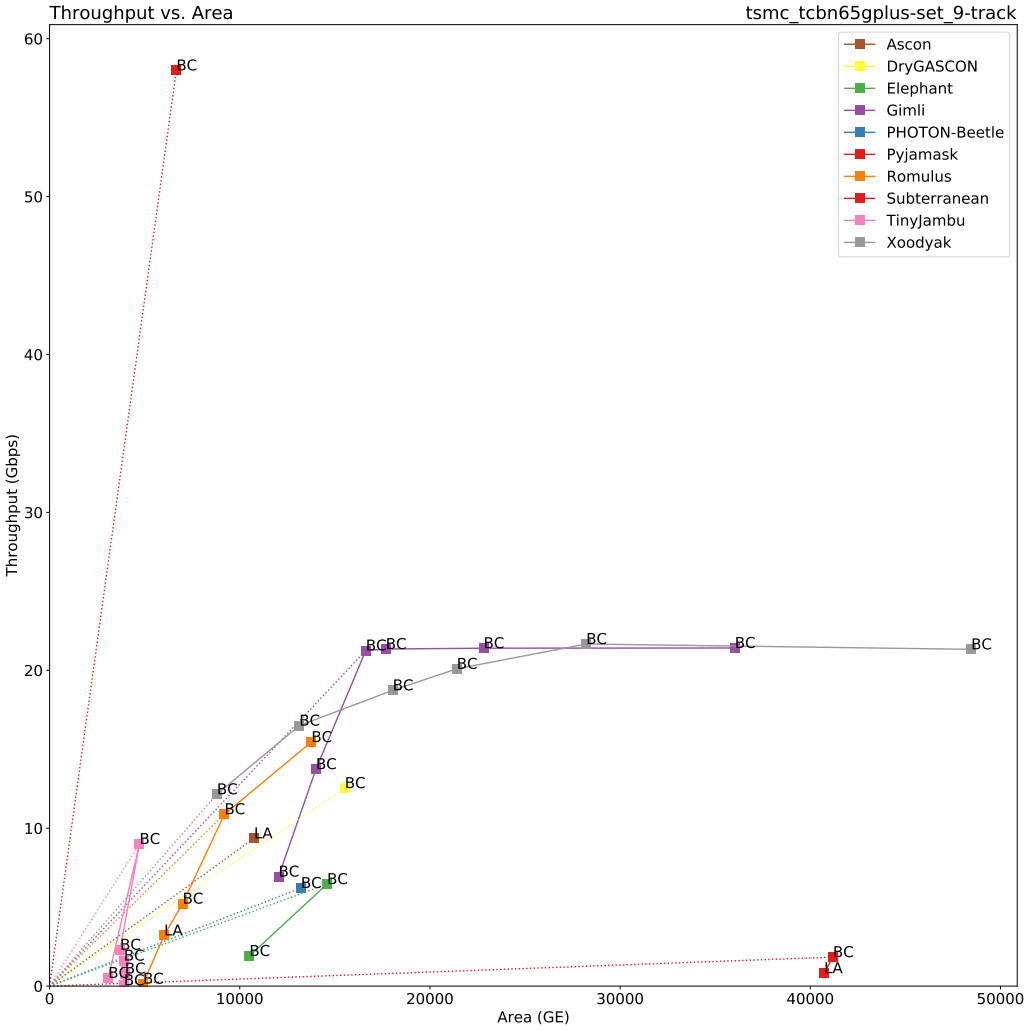

Figure 42: Throughput vs. Area for |A| = |M| = 1536 bytes on TSMC 65nm.

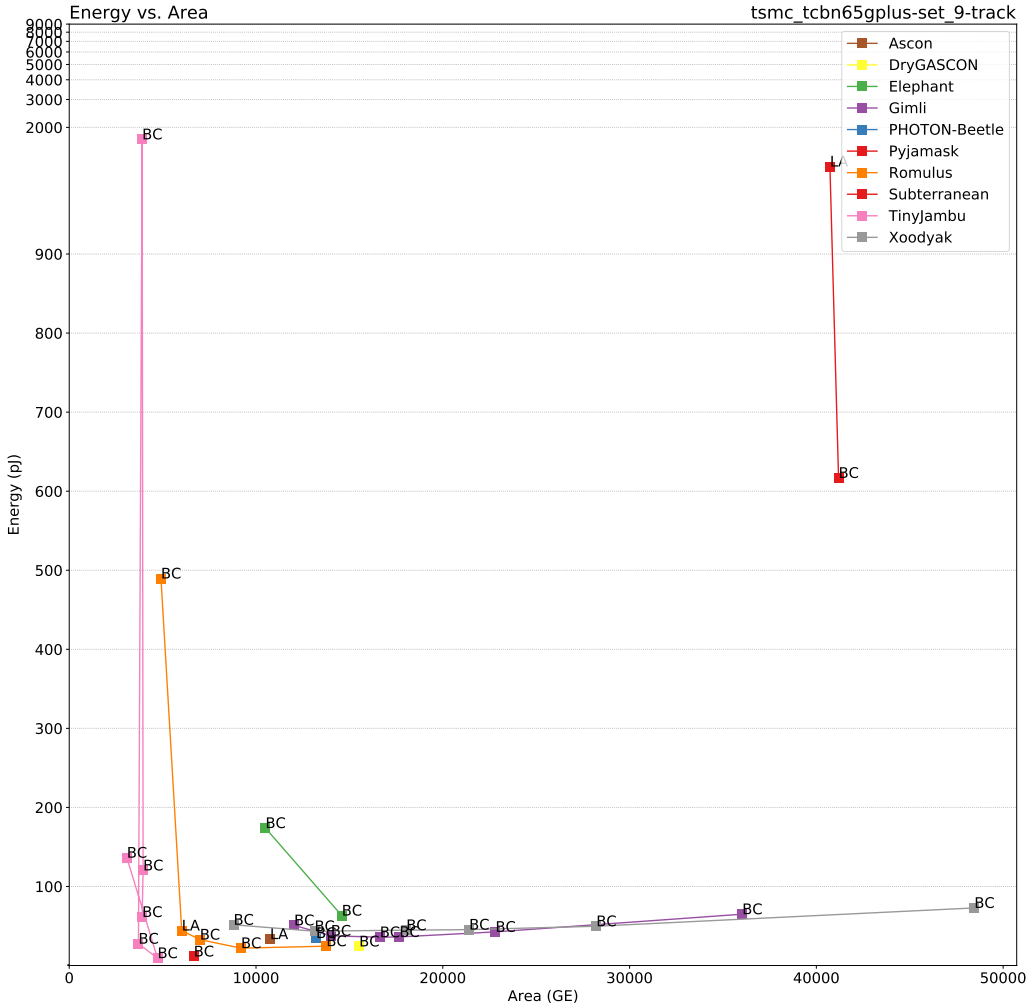

Figure 43: Energy vs. Area for $|A| = 16$ bytes on TSMC 65nm. The energy axis follows a log scale for values $\geqslant 900$ pJ.

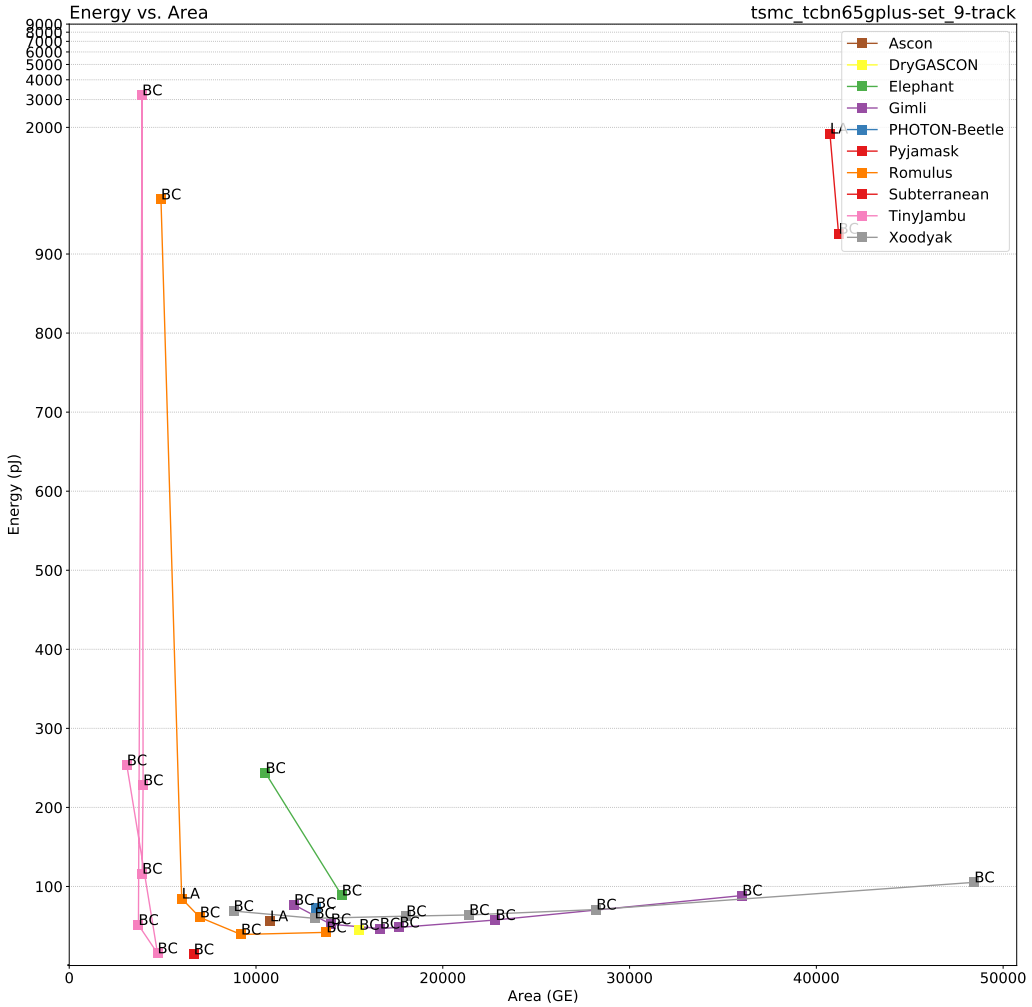

Figure 44: Energy vs. Area for $|A| = 64$ bytes on TSMC 65nm. The energy axis follows a log scale for values $\geqslant 900$ pJ.

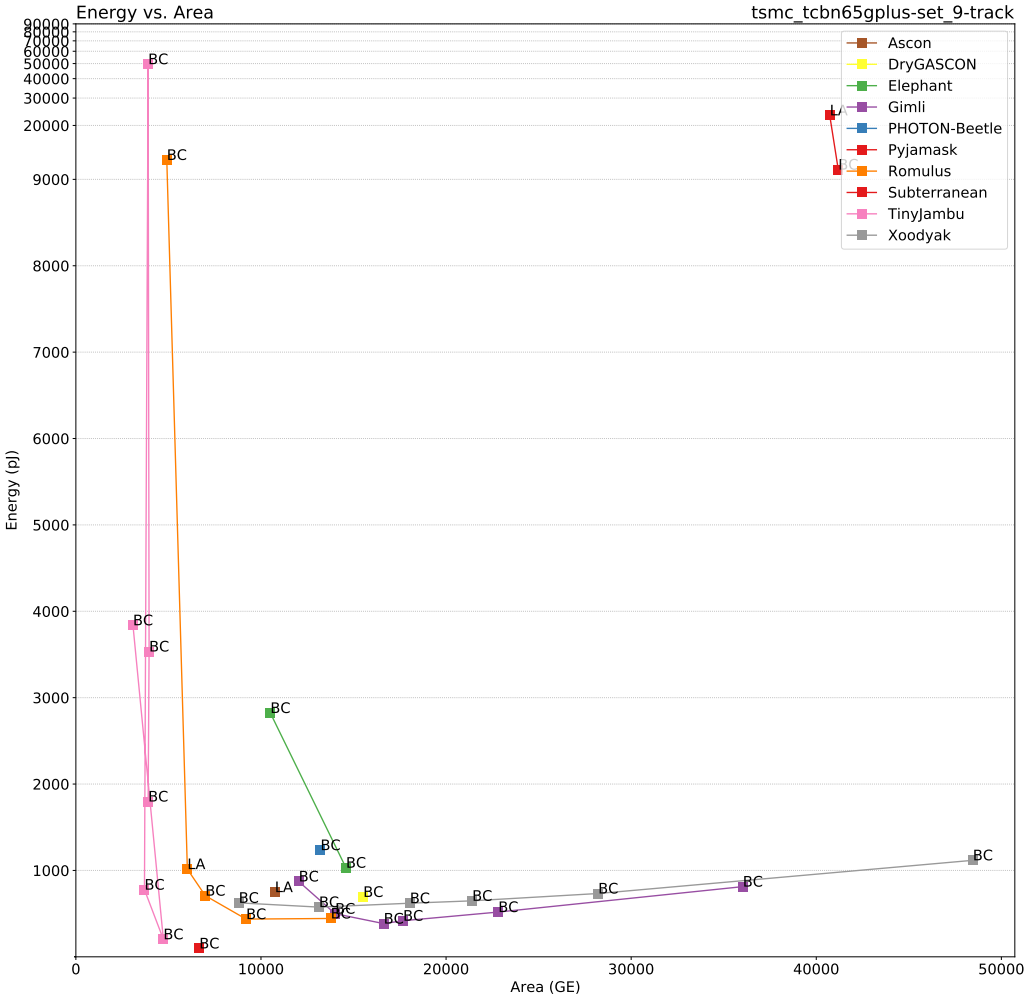

Figure 45: Energy vs. Area for $|A| = 1536$ bytes on TSMC 65nm. The energy axis follows a log scale for values $\geqslant 9000$ pJ.

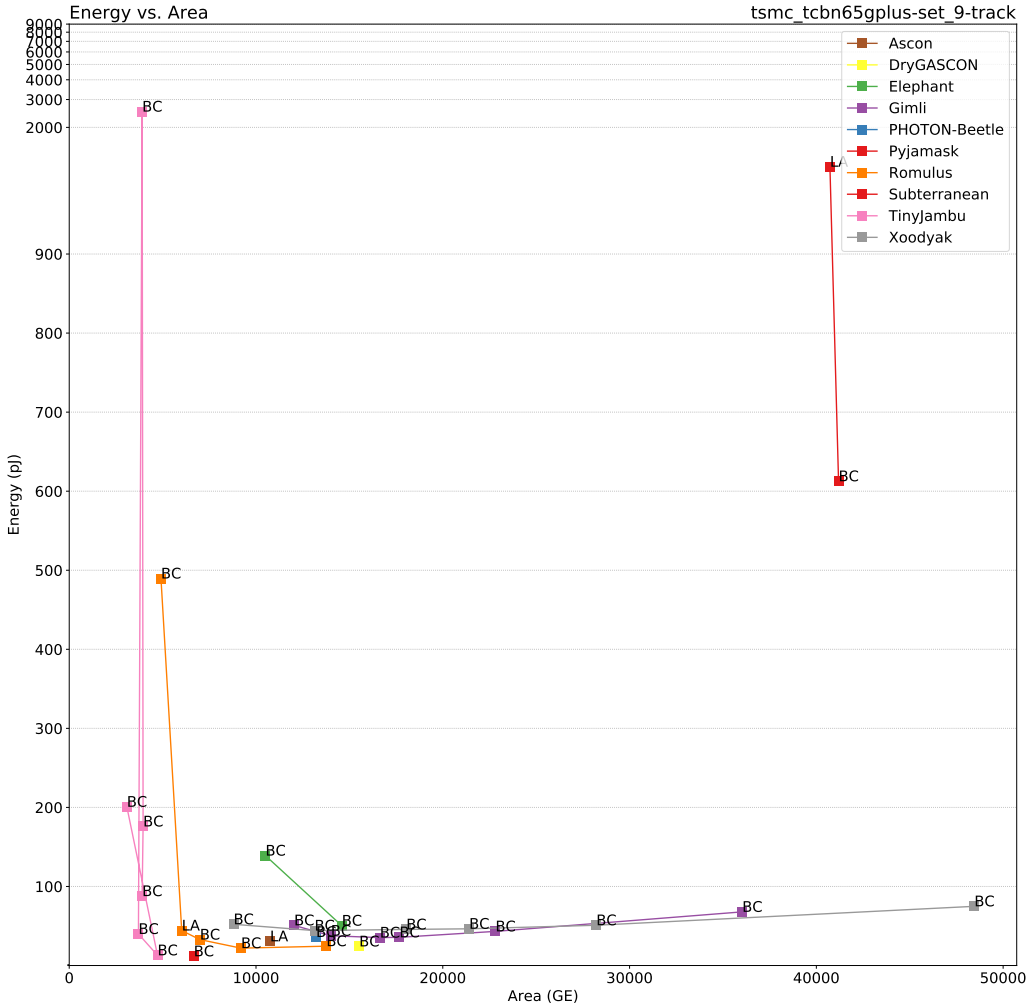

Figure 46: Energy vs. Area for $|\mathrm{M}| = 16$ bytes on TSMC 65nm. The energy axis follows a log scale for values $\geqslant 900$ pJ.

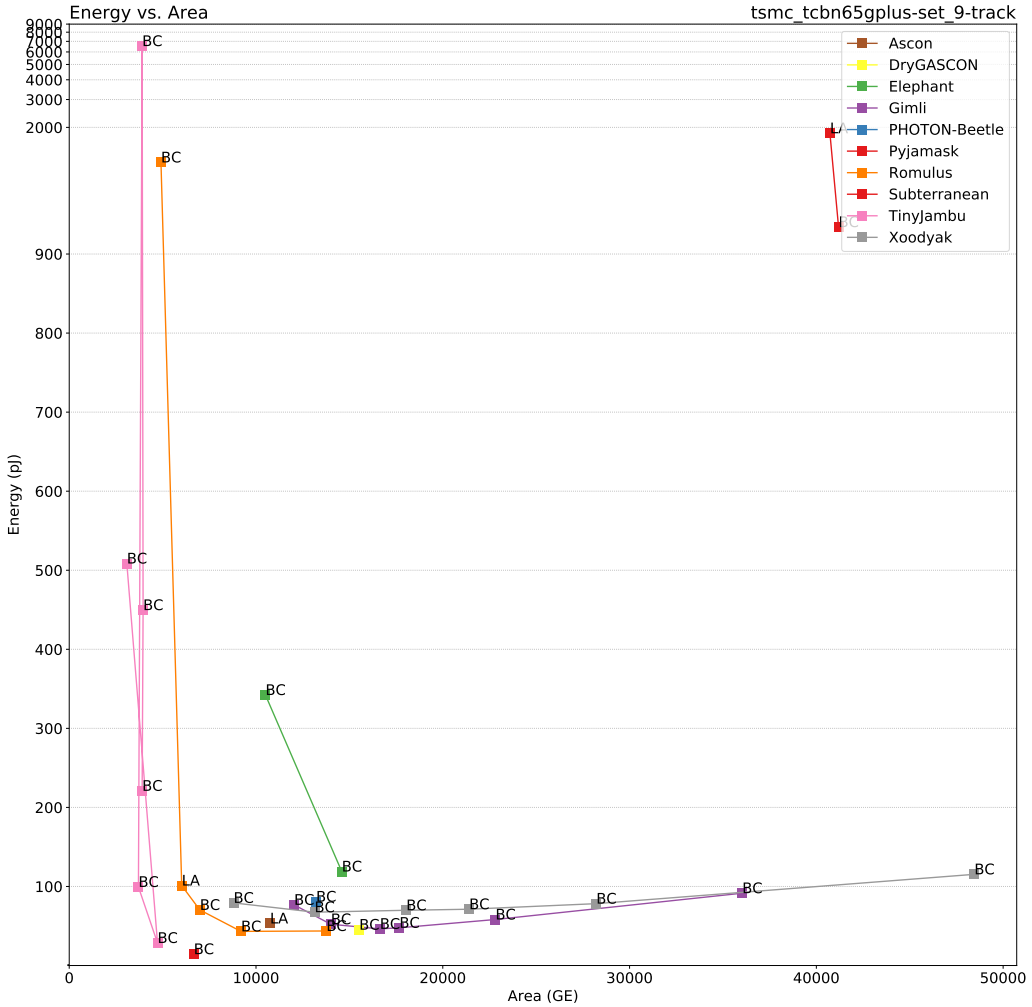

Figure 47: Energy vs. Area for $|M| = 64$ bytes on TSMC 65nm. The energy axis follows a log scale for values $\geqslant 900$ pJ.

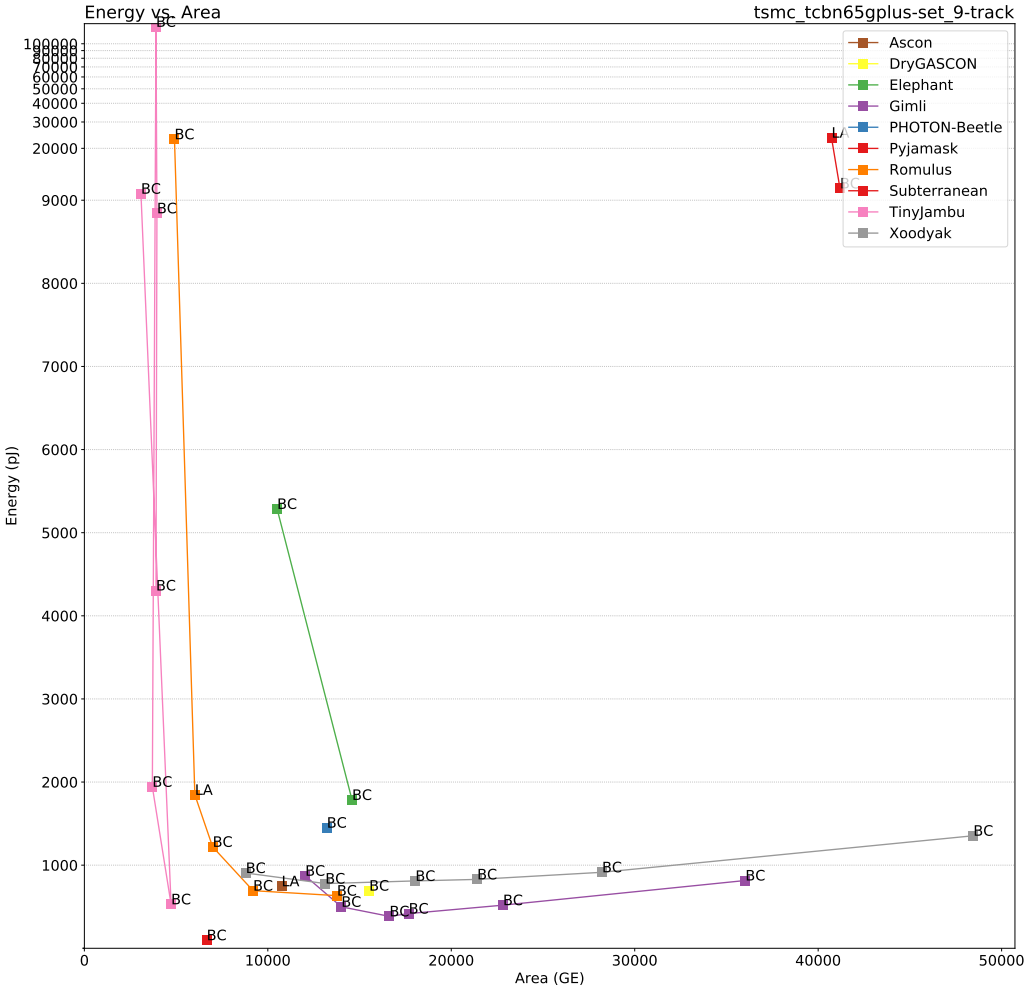

Figure 48: Energy vs. Area for $|M| = 1536$ bytes on TSMC 65nm. The energy axis follows a log scale for values $\geqslant 9000$ pJ.

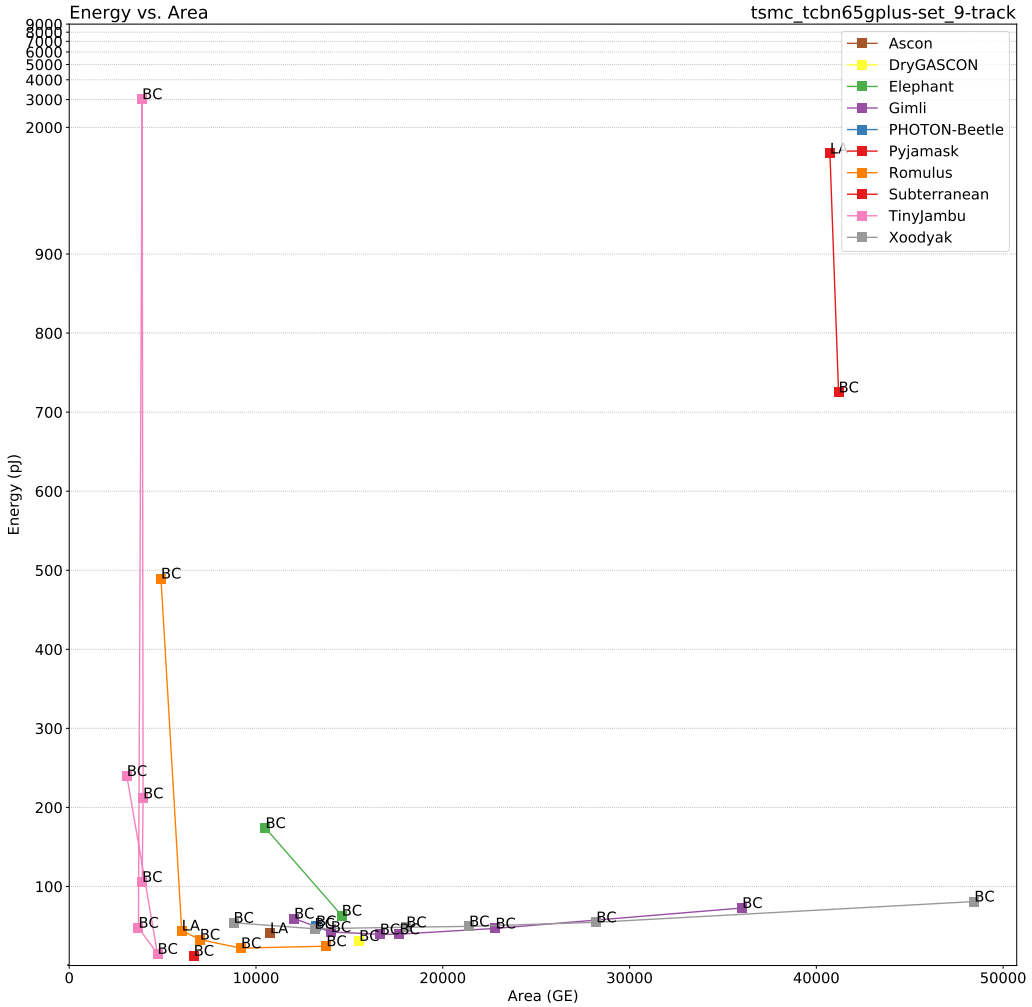

Figure 49: Energy vs. Area for $|A| = |M| = 16$ bytes on TSMC 65nm. The energy axis follows a log scale for values $\geqslant 900$ pJ.

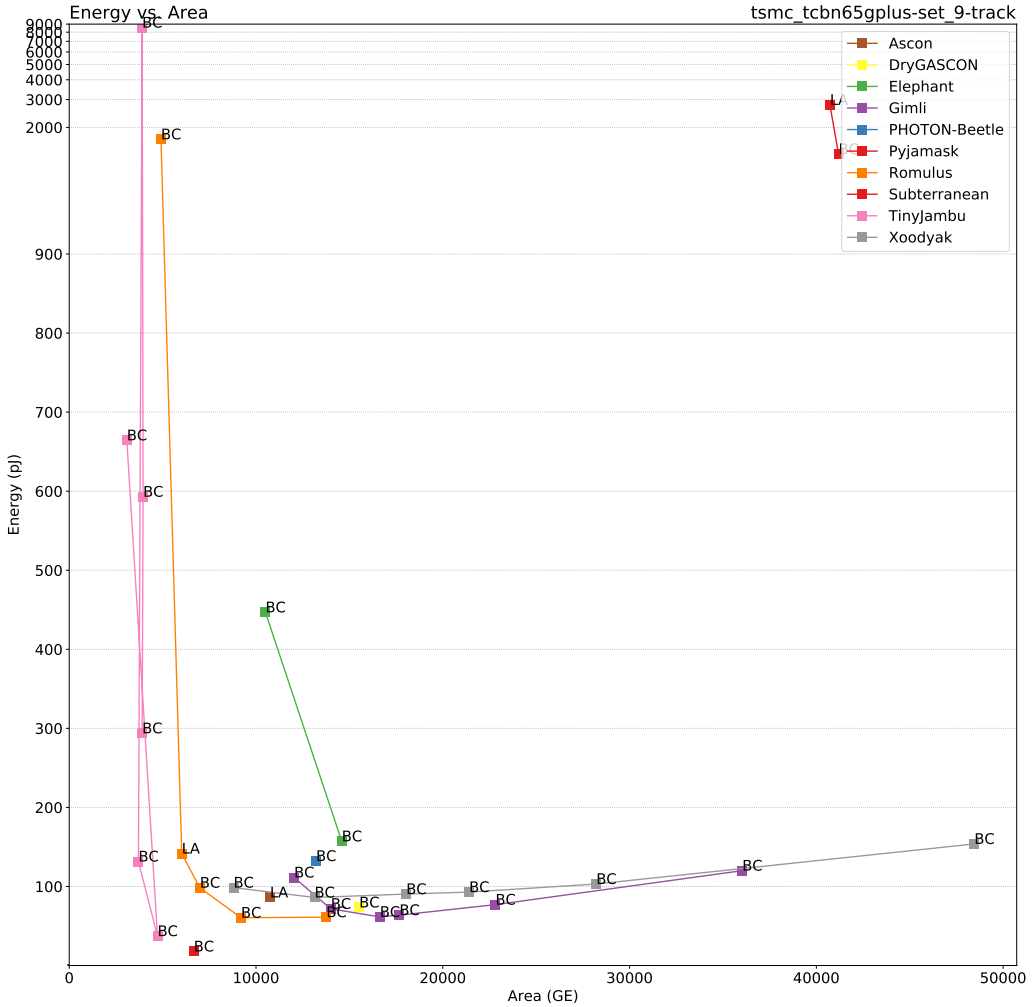

Figure 50: Energy vs. Area for $|A| = |M| = 64$ bytes on TSMC 65nm. The energy axis follows a log scale for values $\geqslant 900$ pJ.

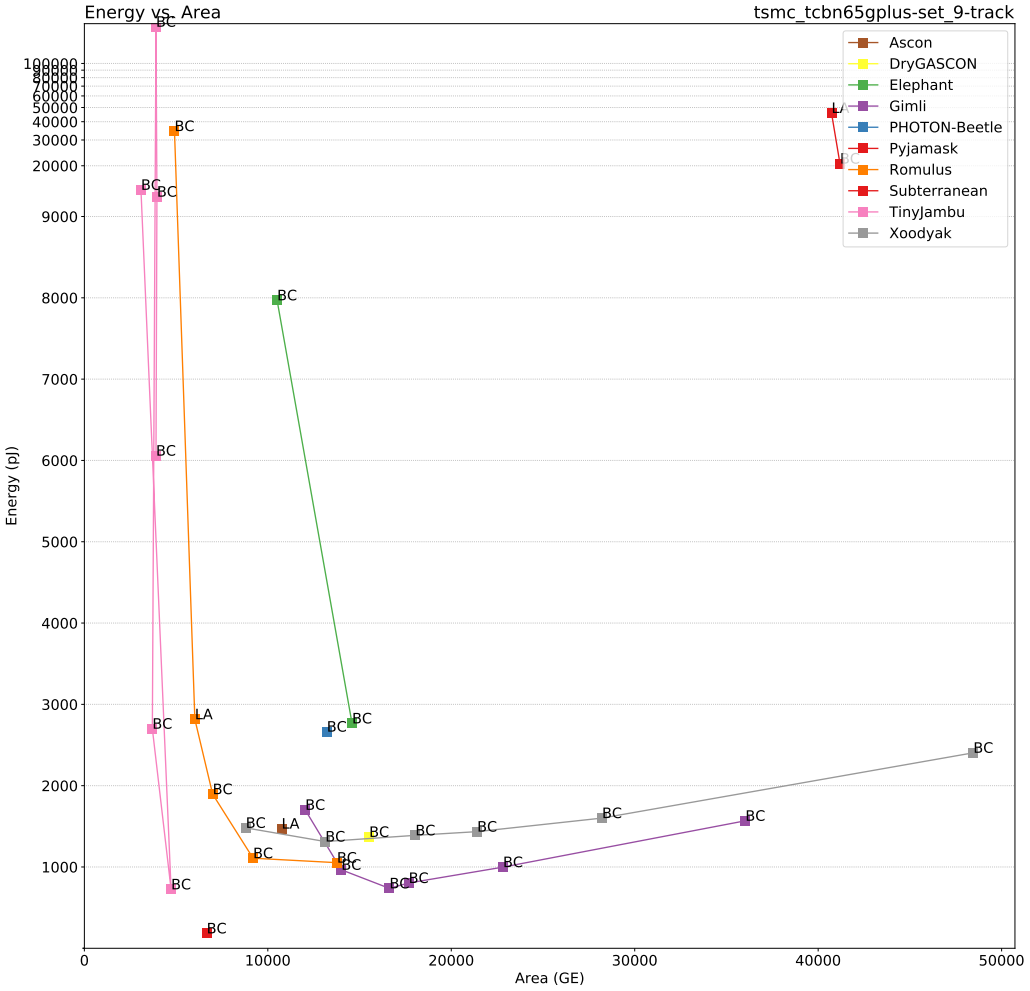

Figure 51: Energy vs. Area for $|A| = |M| = 1536$ bytes on TSMC 65nm. The energy axis follows a log scale for values $\geqslant 9000$ pJ.

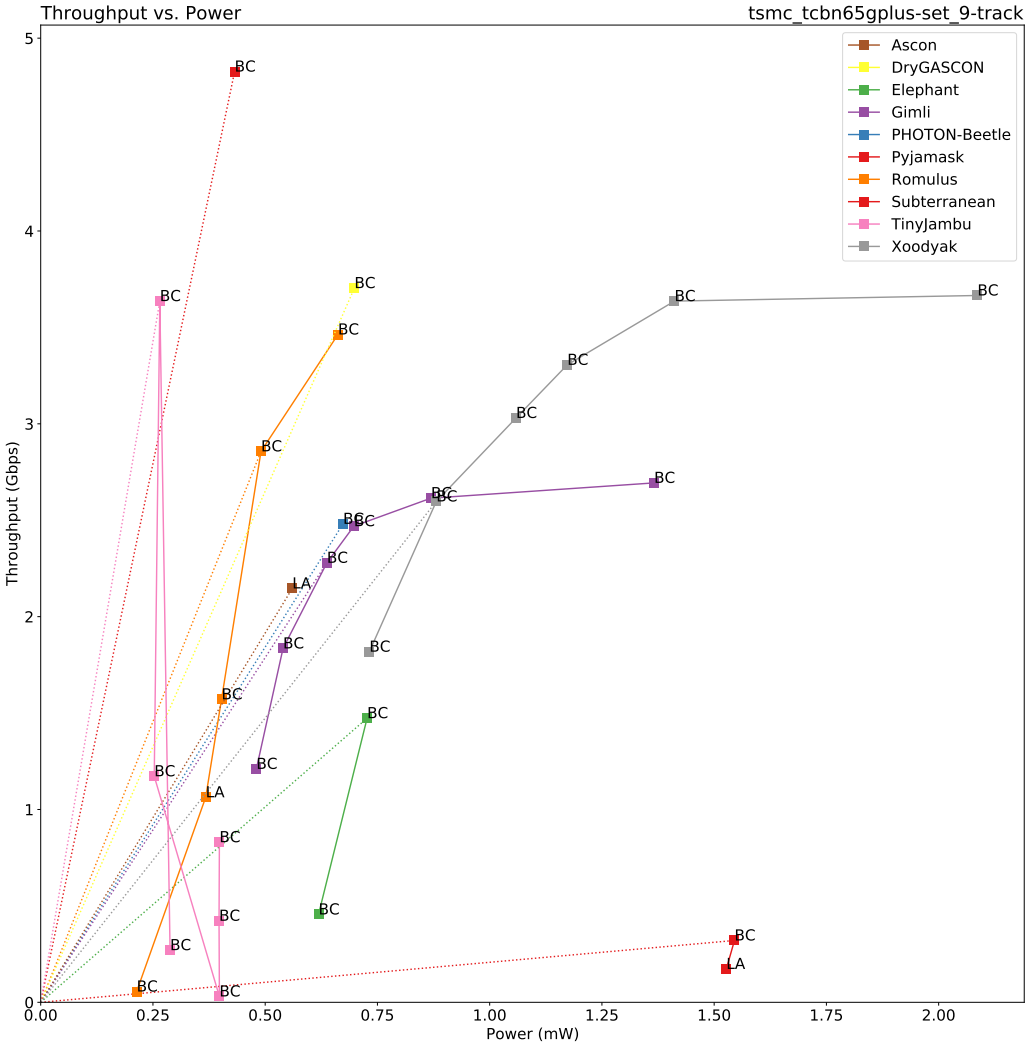

Figure 52: Throughput vs. Power for $|A| = 16$ bytes on TSMC 65nm.

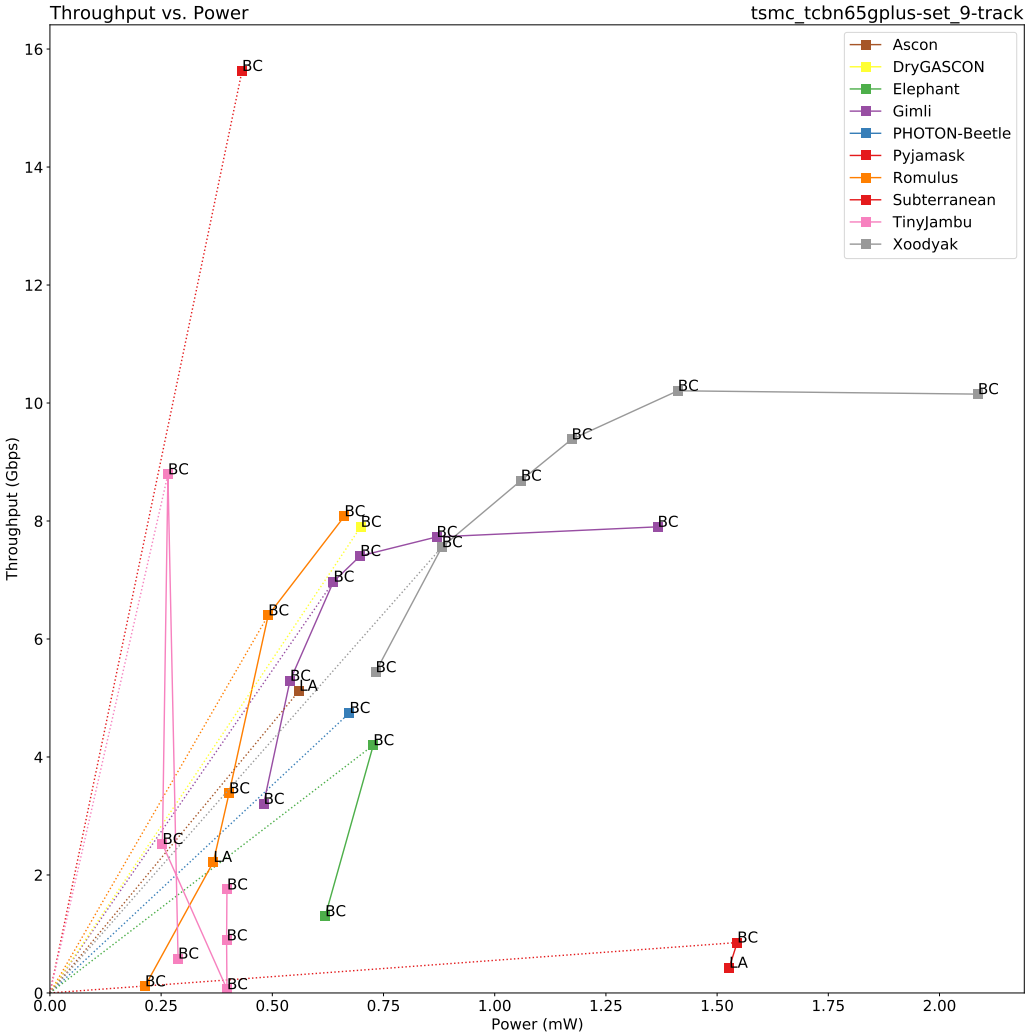

Figure 53: Throughput vs. Power for $|A| = 64$ bytes on TSMC 65nm.

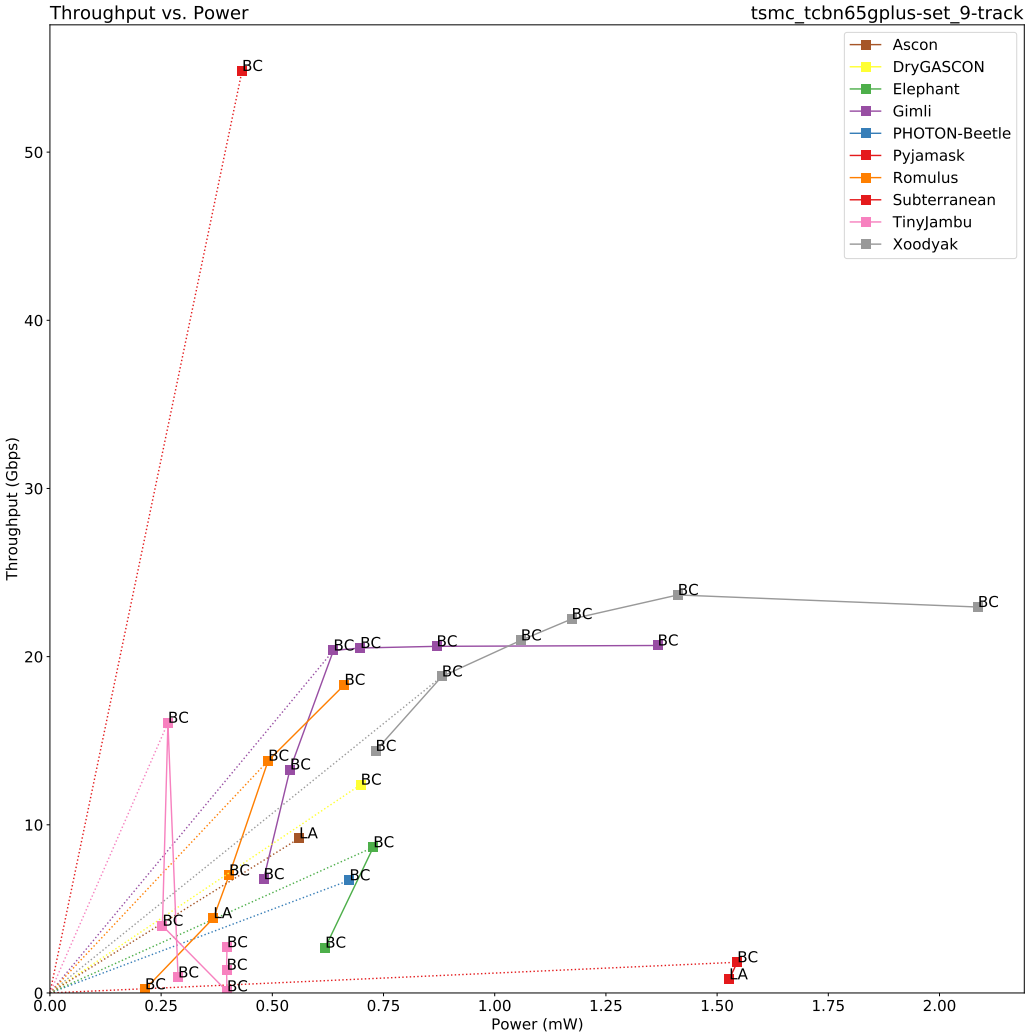

Figure 54: Throughput vs. Power for |A| = 1536 bytes on TSMC 65nm.

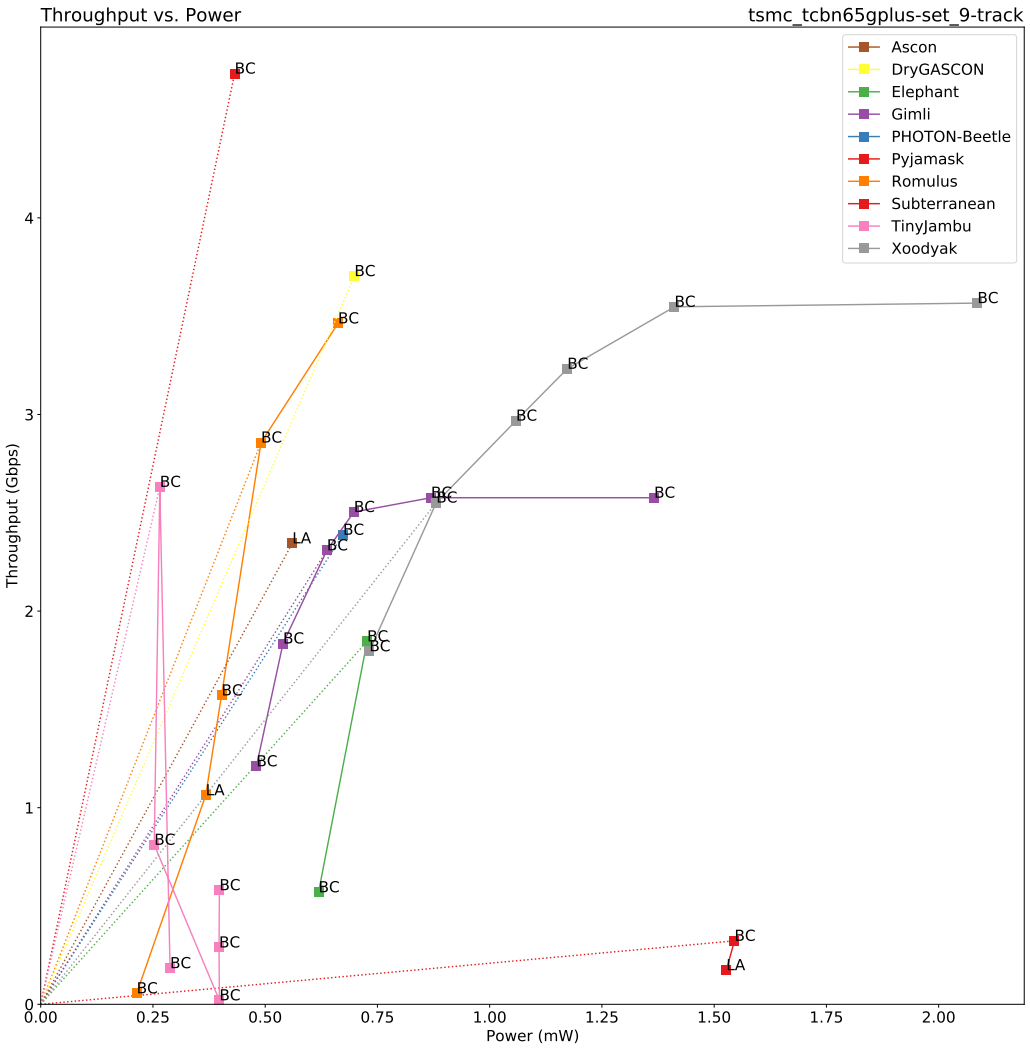

Figure 55: Throughput vs. Power for |M| = 16 bytes on TSMC 65nm.

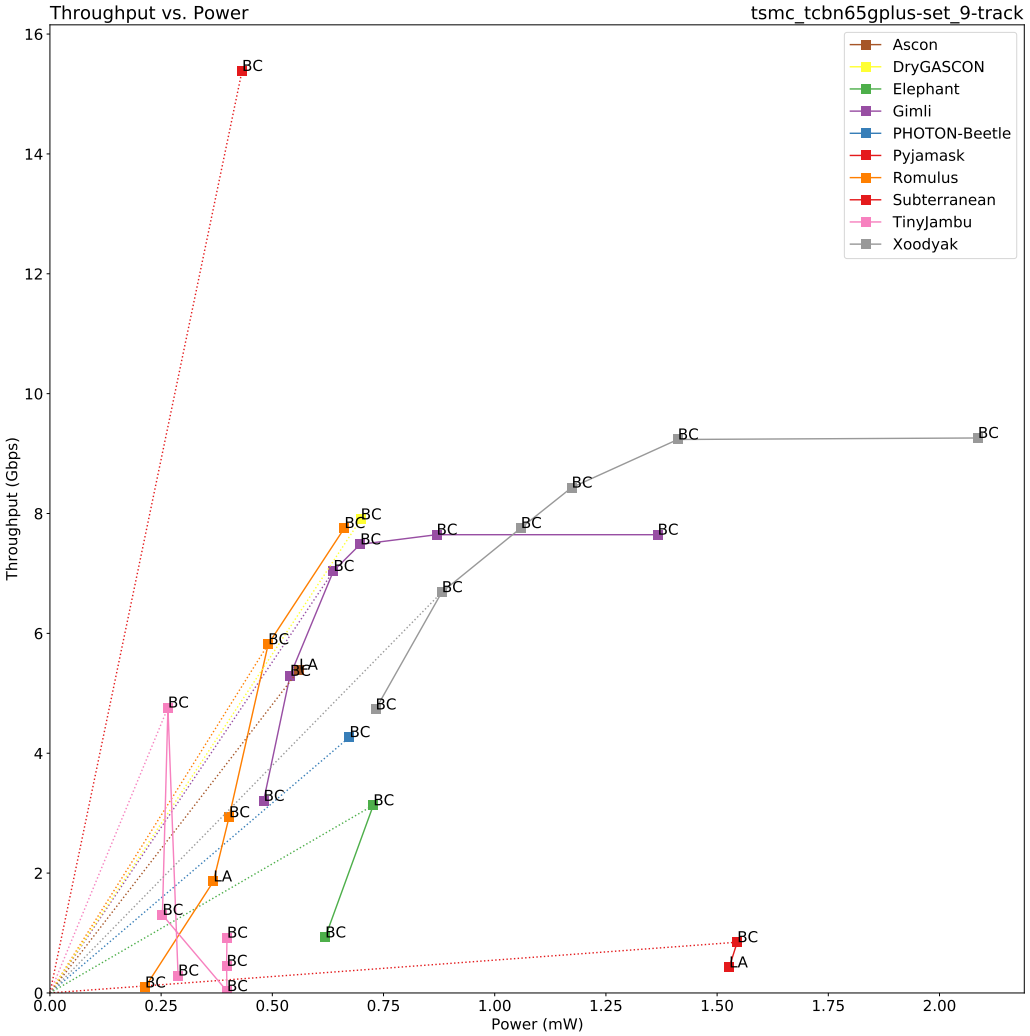

Figure 56: Throughput vs. Power for |M| = 64 bytes on TSMC 65nm.

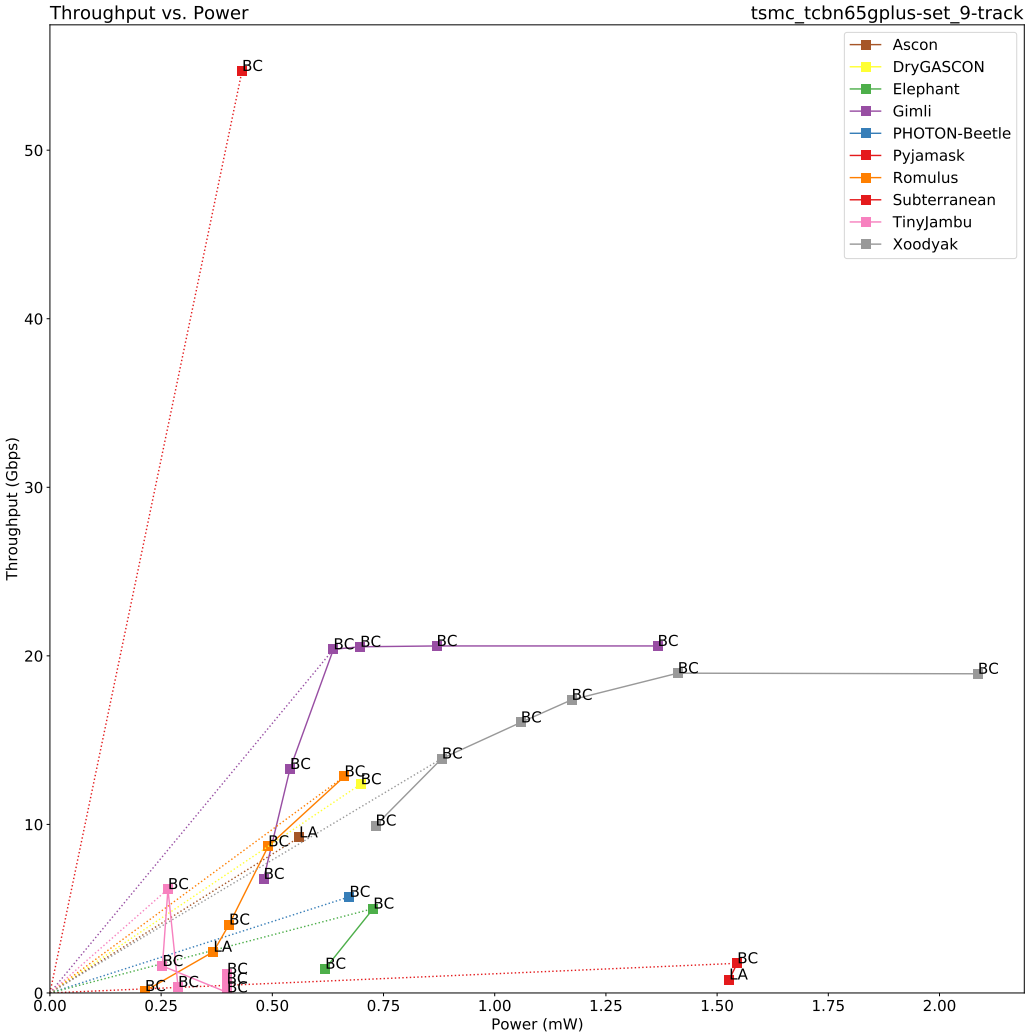

Figure 57: Throughput vs. Power for $|M| = 1536$ bytes on TSMC 65nm.

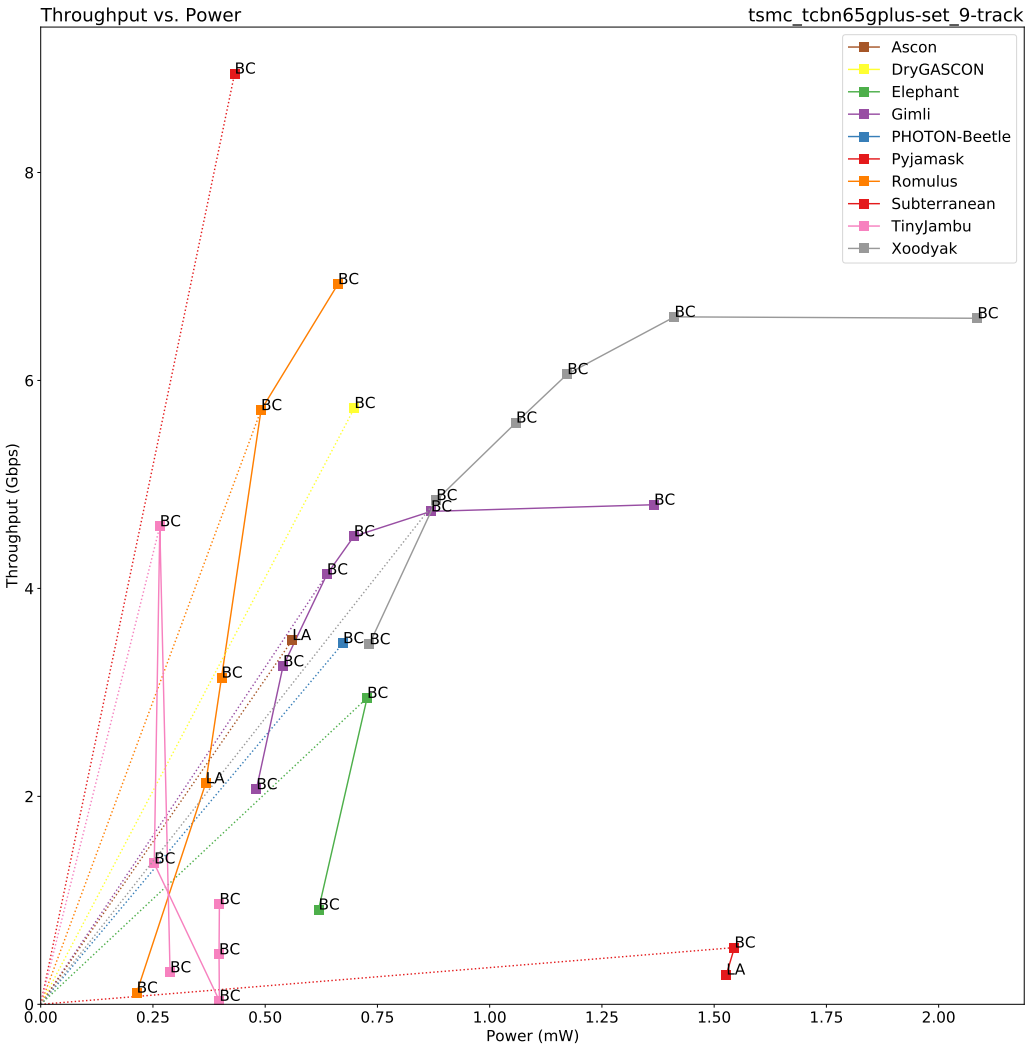

Figure 58: Throughput vs. Power for $|A| = |M| = 16$ bytes on TSMC 65nm.

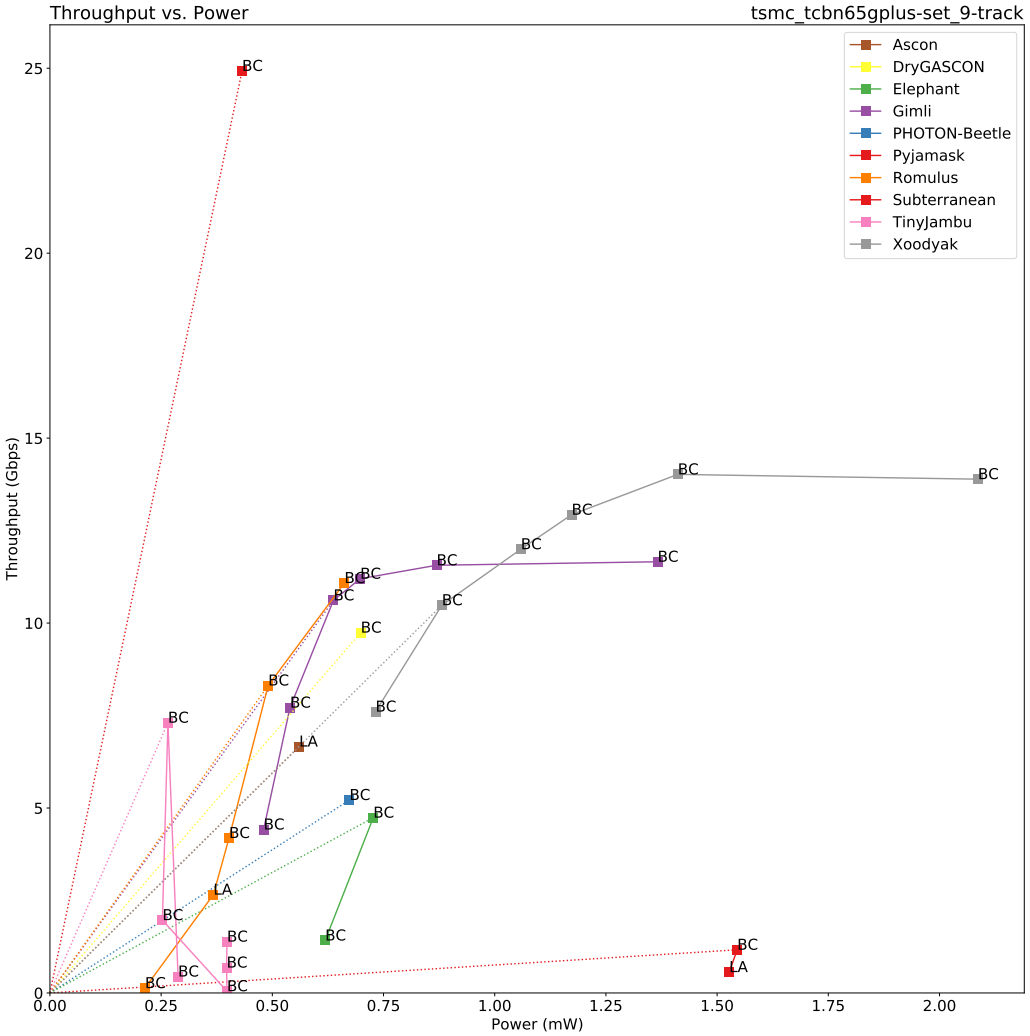

Figure 59: Throughput vs. Power for $|A| = |M| = 64$ bytes on TSMC 65nm.

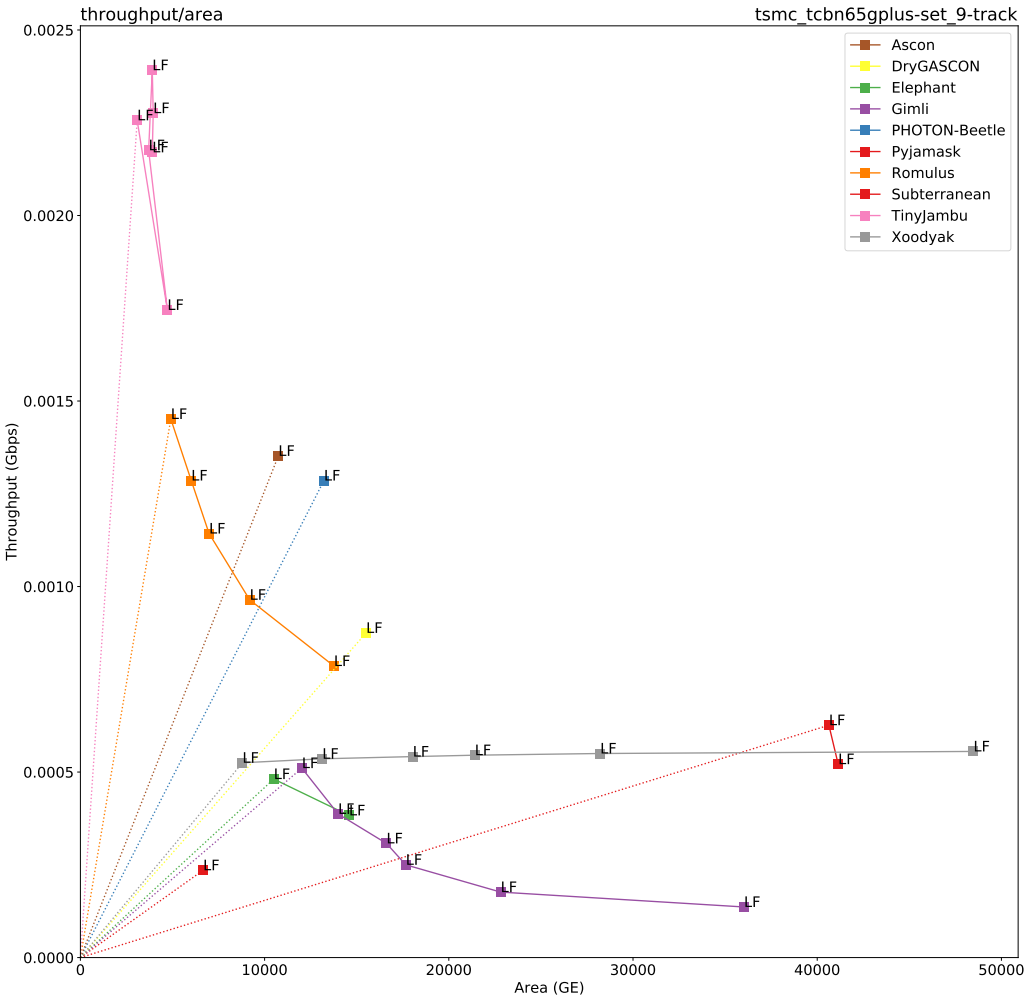

Figure 60: 3 Mbps: Throughput vs. Area for |A| = 16 bytes on TSMC 65nm.

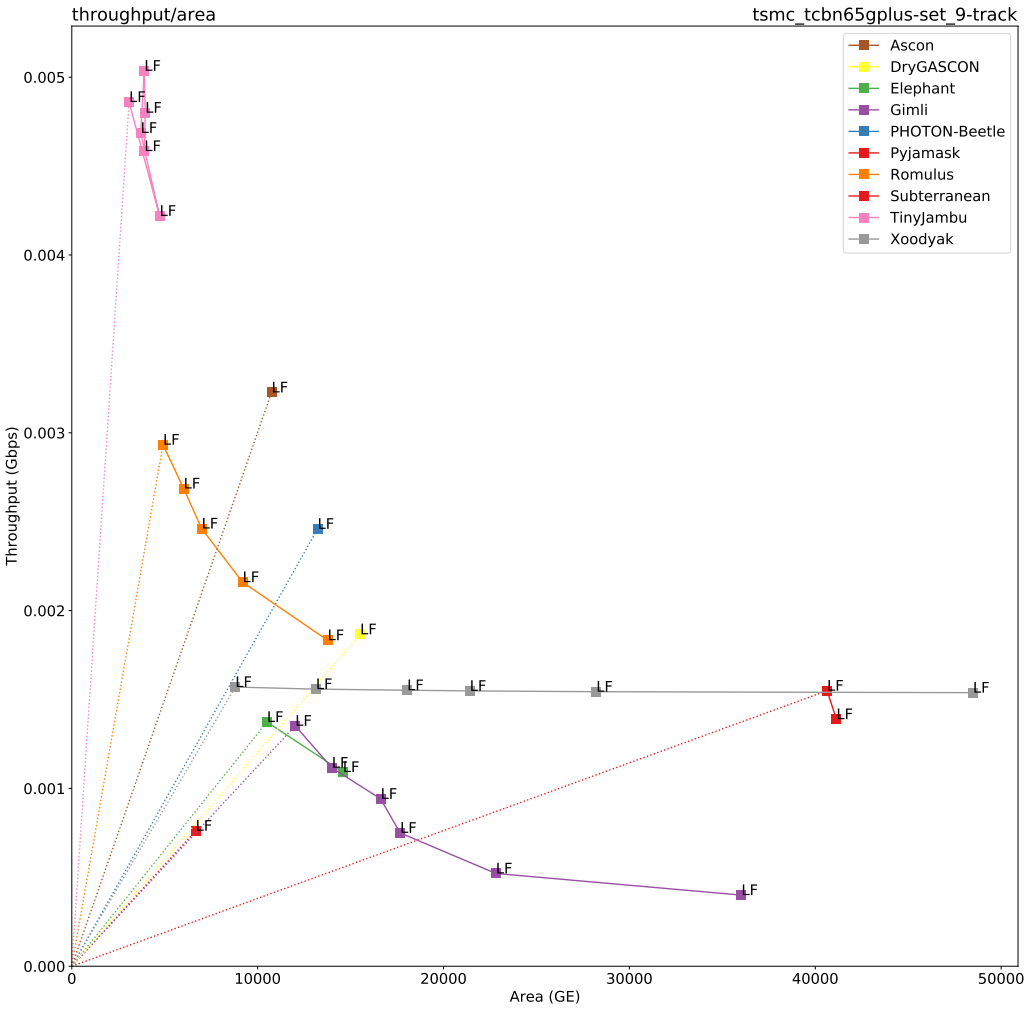

Figure 61: 3 Mbps: Throughput vs. Area for |A| = 64 bytes on TSMC 65nm.

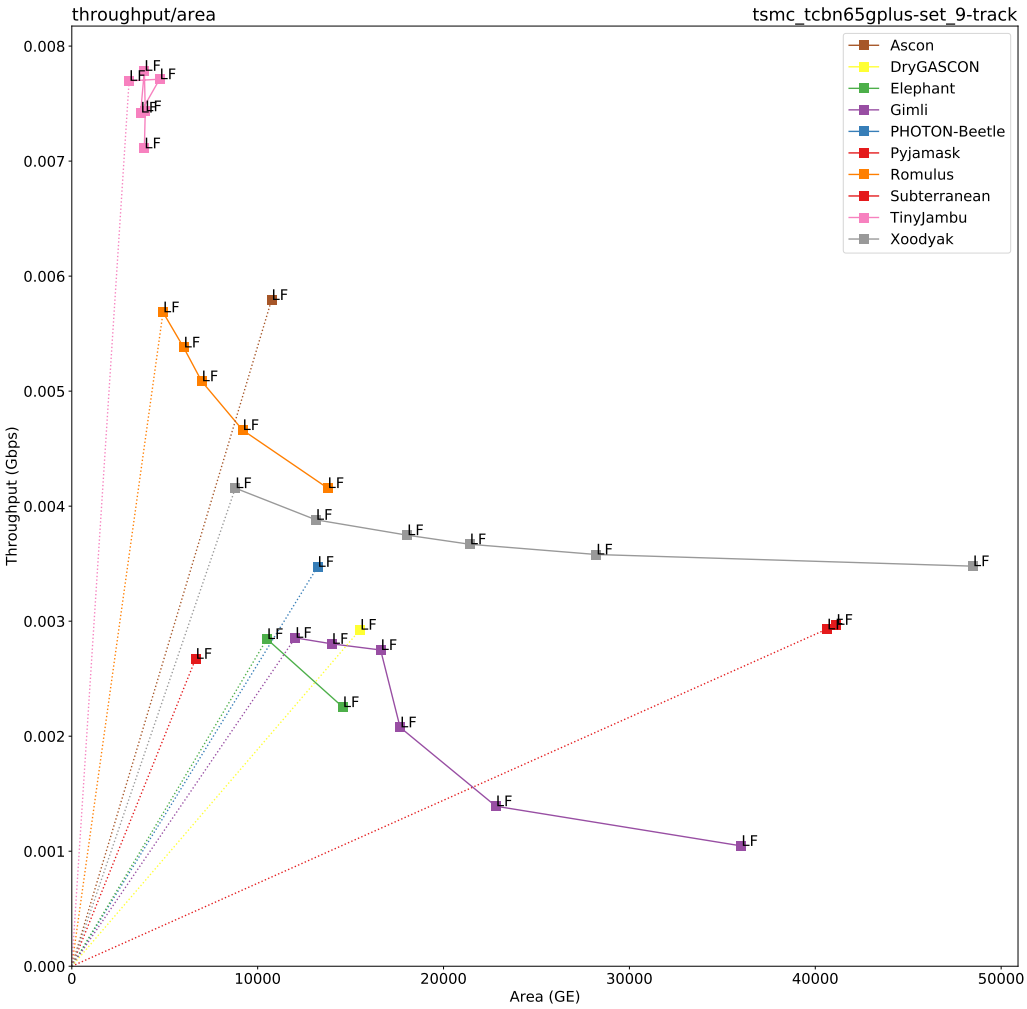

Figure 62: 3 Mbps: Throughput vs. Area for |A| = 1536 bytes on TSMC 65nm.

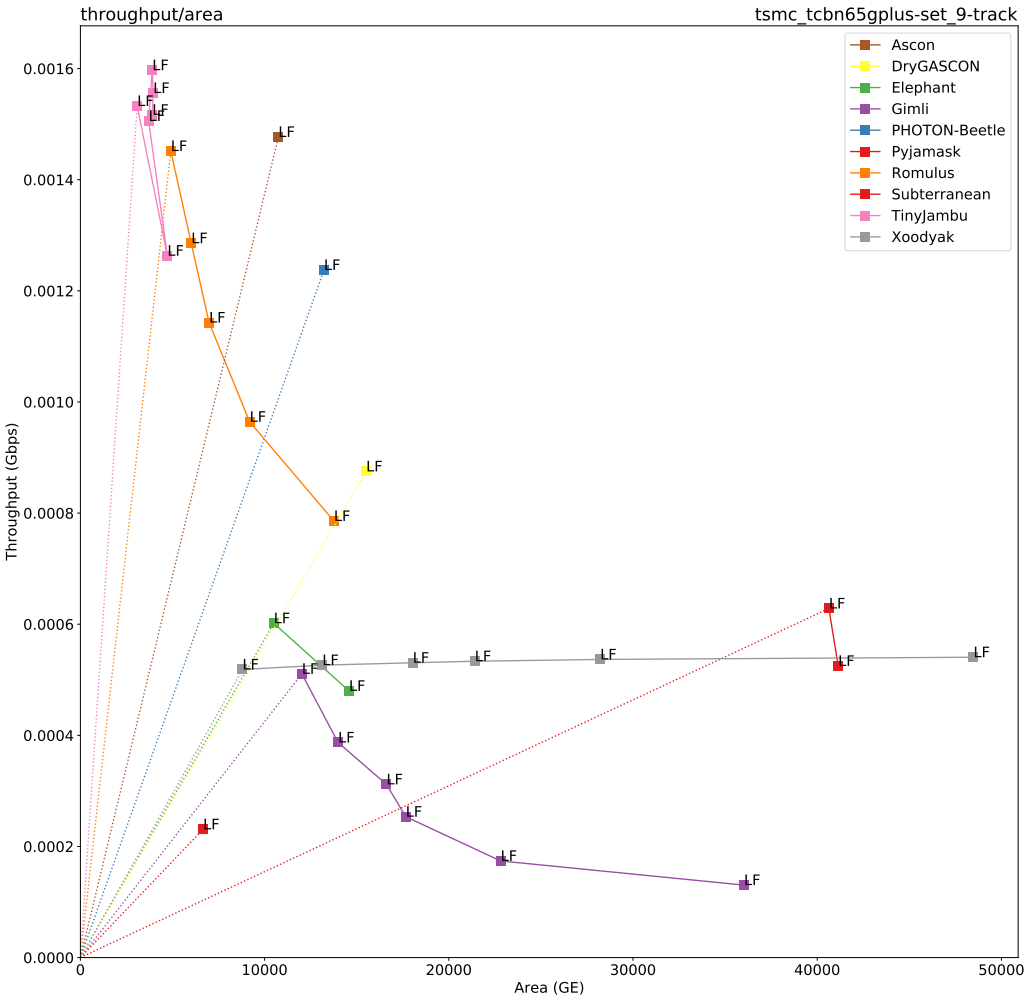

Figure 63: 3 Mbps: Throughput vs. Area for |M| = 16 bytes on TSMC 65nm.

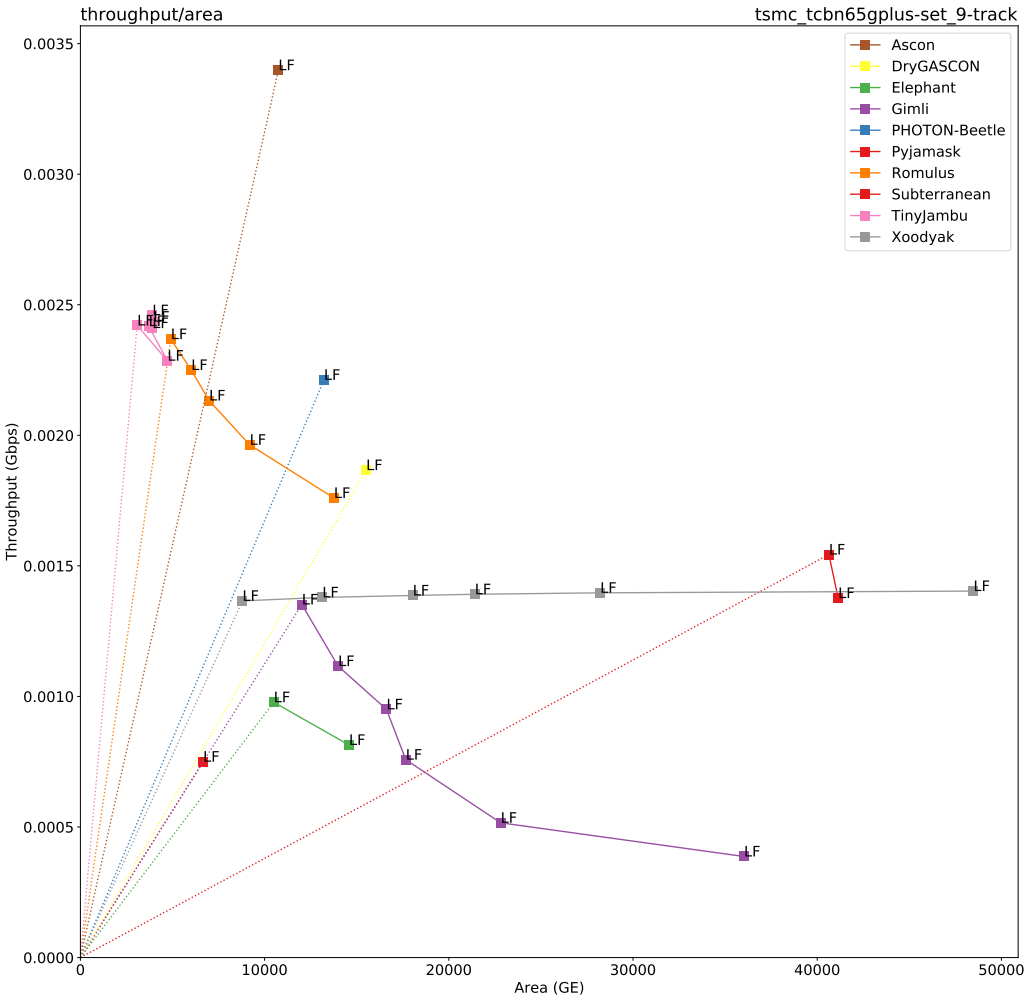

Figure 64: 3 Mbps: Throughput vs. Area for |M| = 64 bytes on TSMC 65nm.

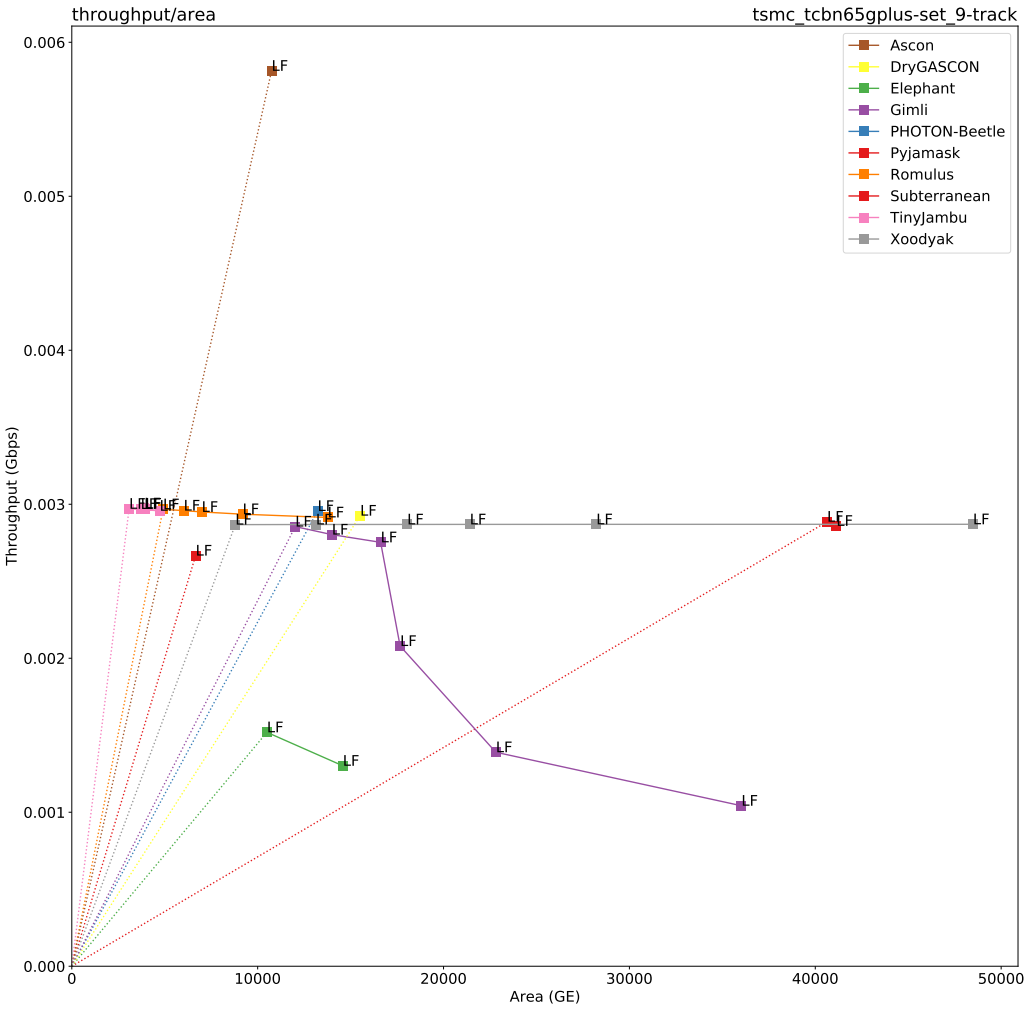

Figure 65: 3 Mbps: Throughput vs. Area for |M| = 1536 bytes on TSMC 65nm.

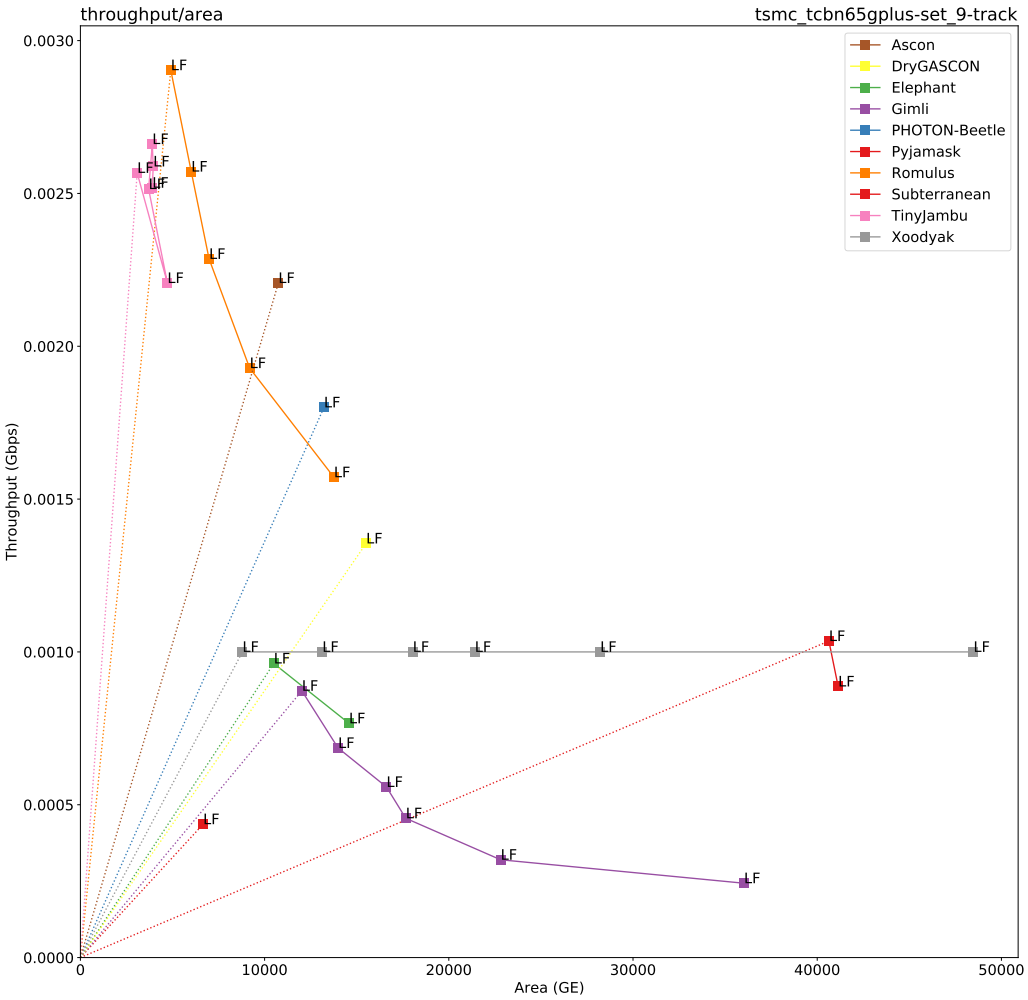

Figure 66: 3 Mbps: Throughput vs. Area for $|A| = |M| = 16$ bytes on TSMC 65nm.

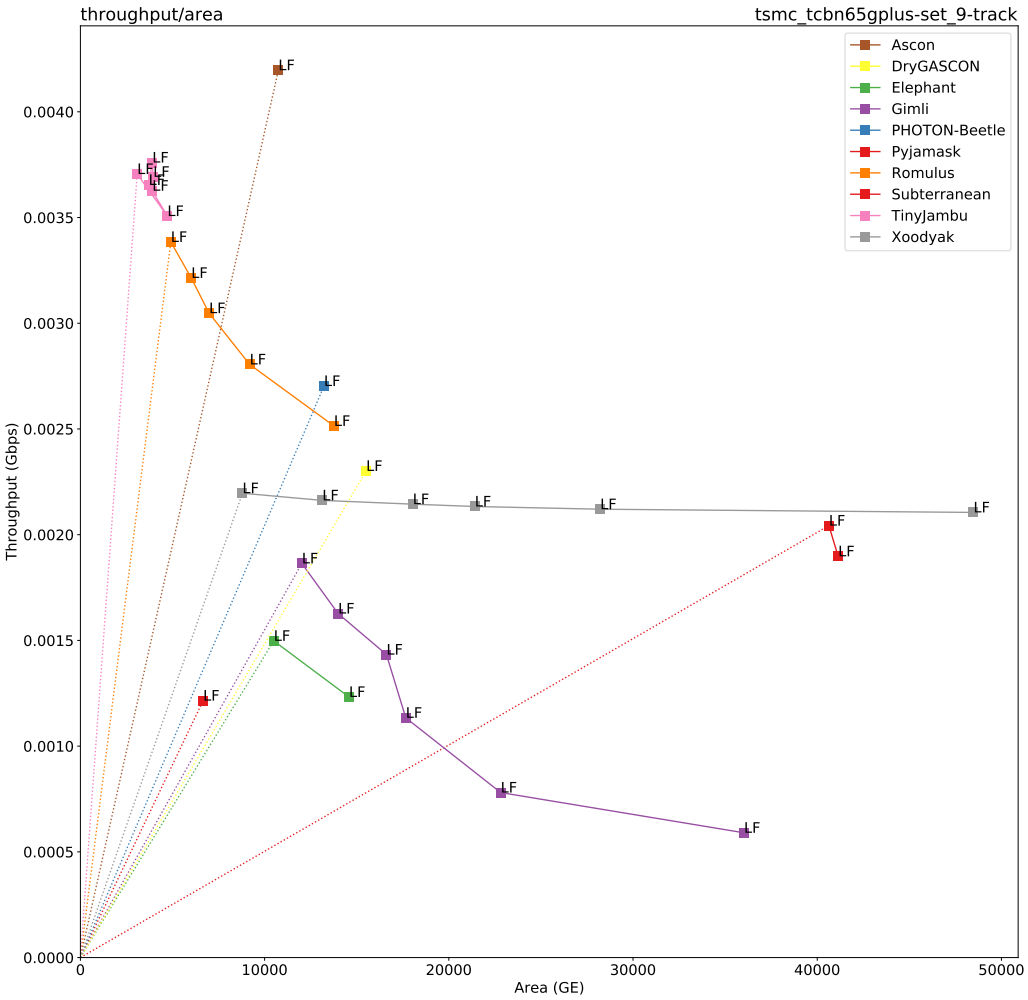

Figure 67: 3 Mbps: Throughput vs. Area for $|A| = |M| = 64$ bytes on TSMC 65nm.

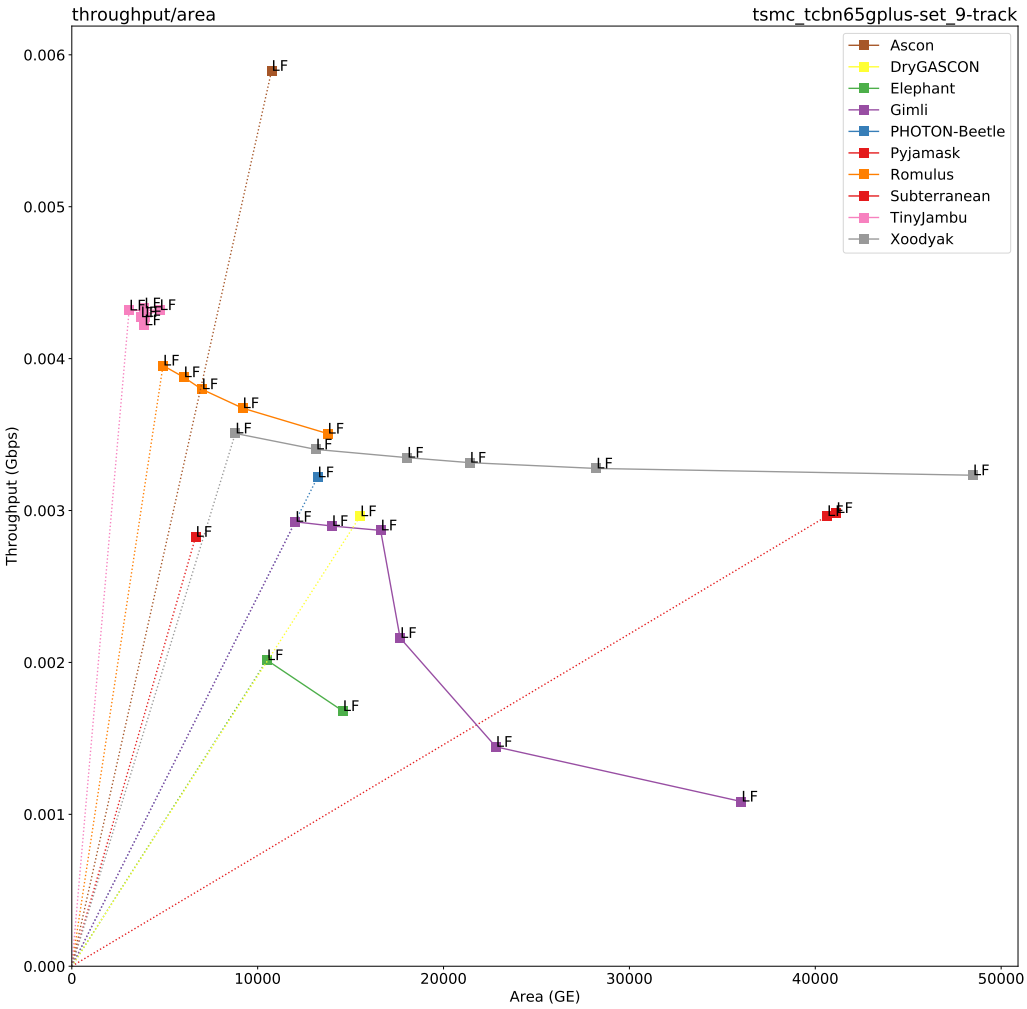

Figure 68: 3 Mbps: Throughput vs. Area for $|A| = |M| = 1536$ bytes on TSMC 65nm.

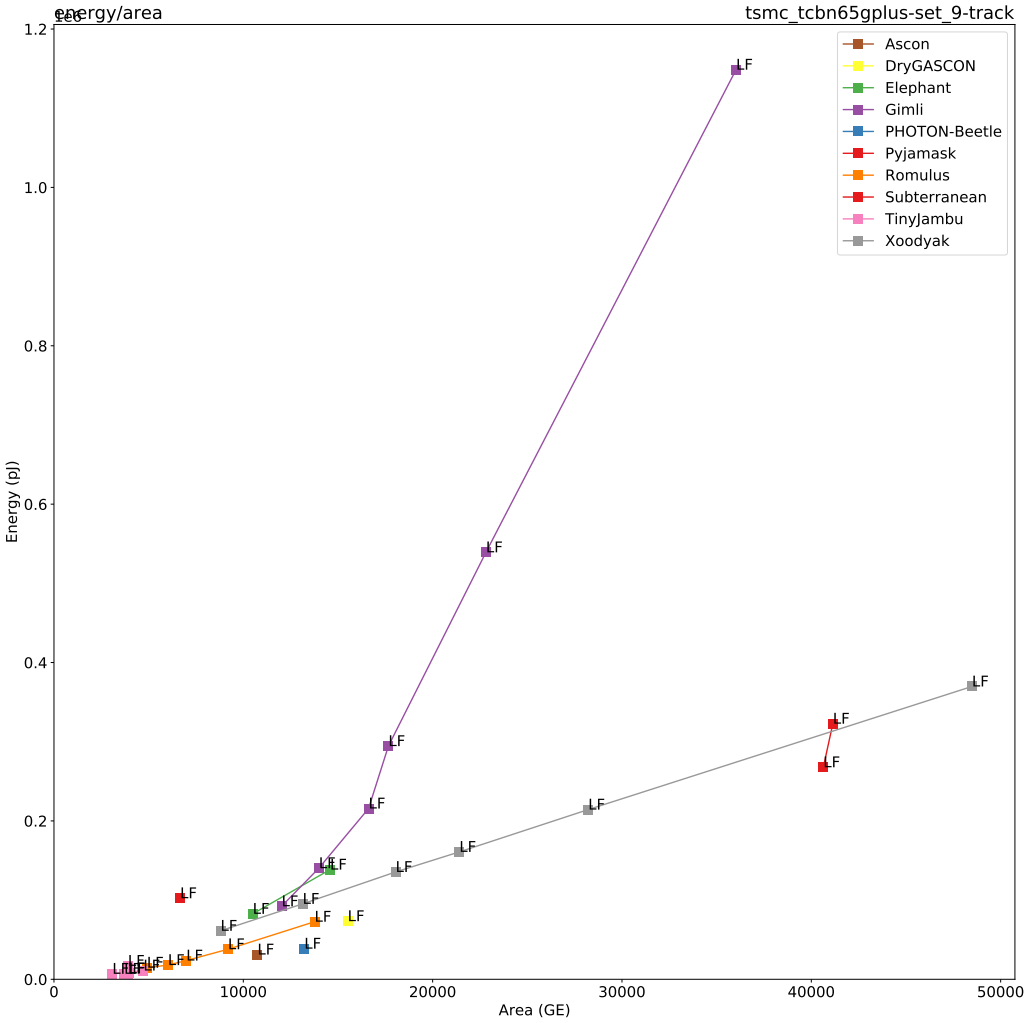

Figure 69: 3 Mbps: Energy vs. Area for $|A| = 16$ bytes on TSMC 65nm.

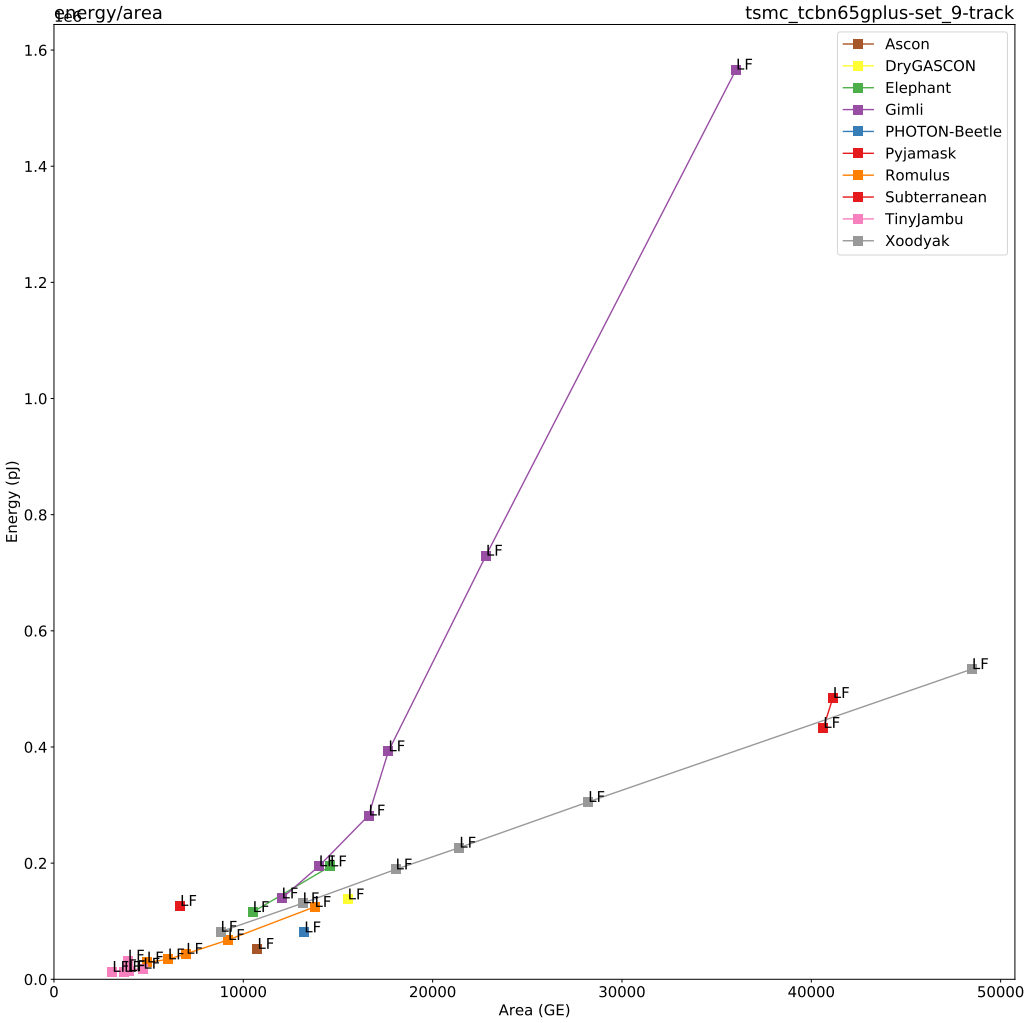

Figure 70: 3 Mbps: Energy vs. Area for $|A| = 64$ bytes on TSMC 65nm.

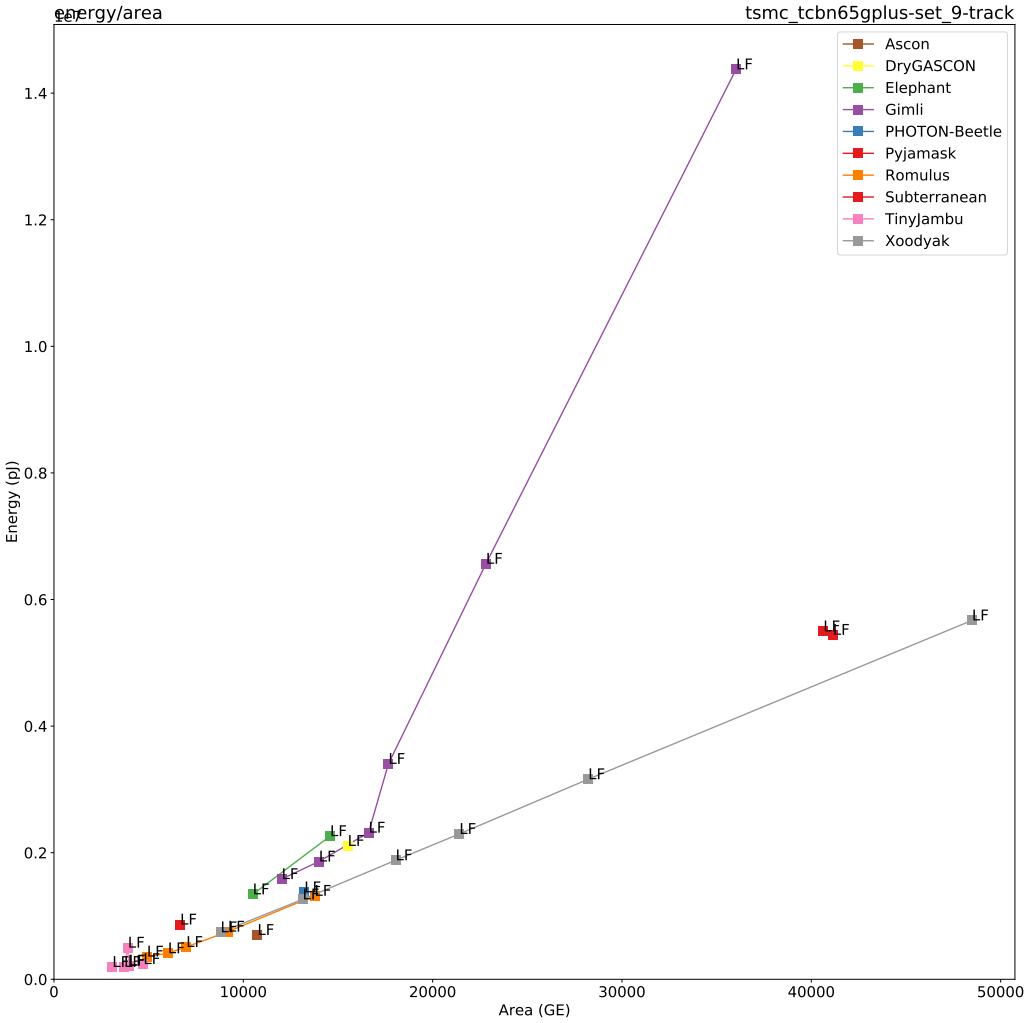

Figure 71: 3 Mbps: Energy vs. Area for $|A| = 1536$ bytes on TSMC 65nm.

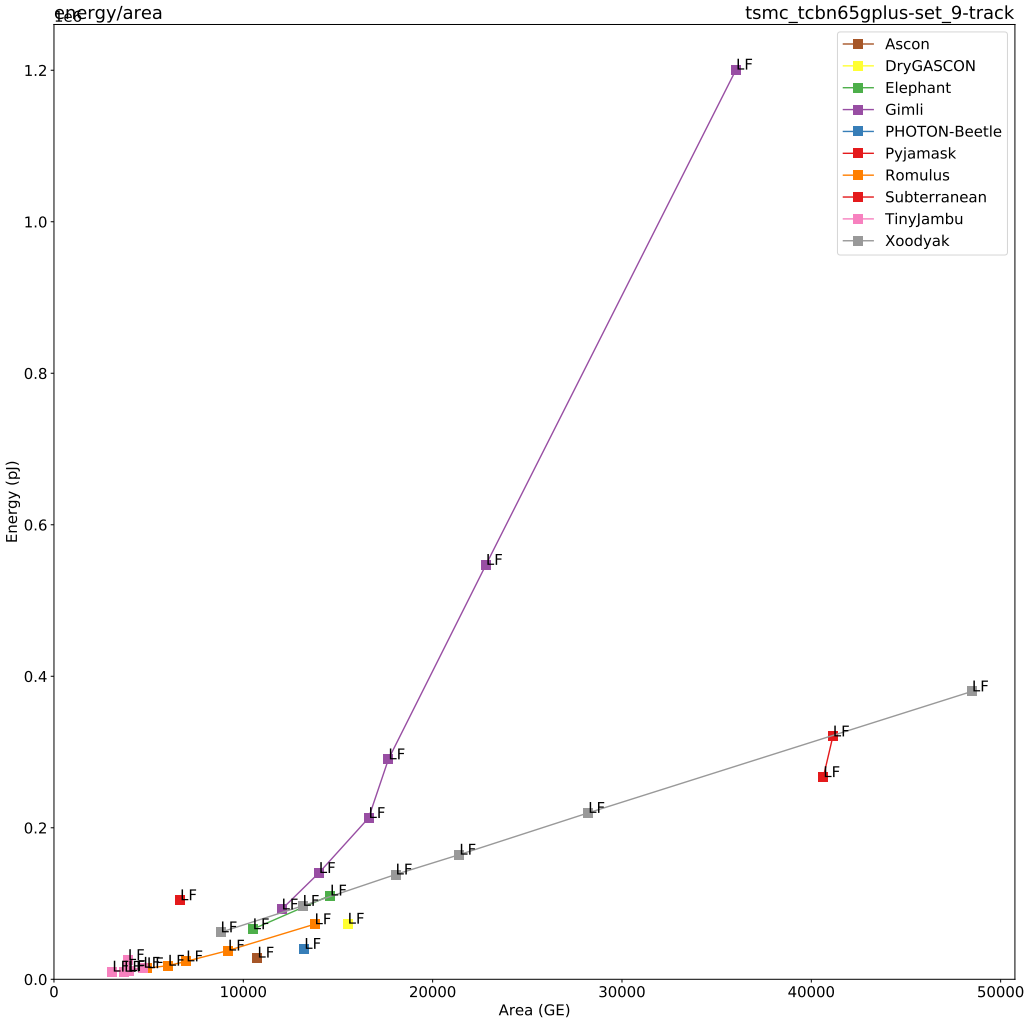

Figure 72: 3 Mbps: Energy vs. Area for |M| = 16 bytes on TSMC 65nm.

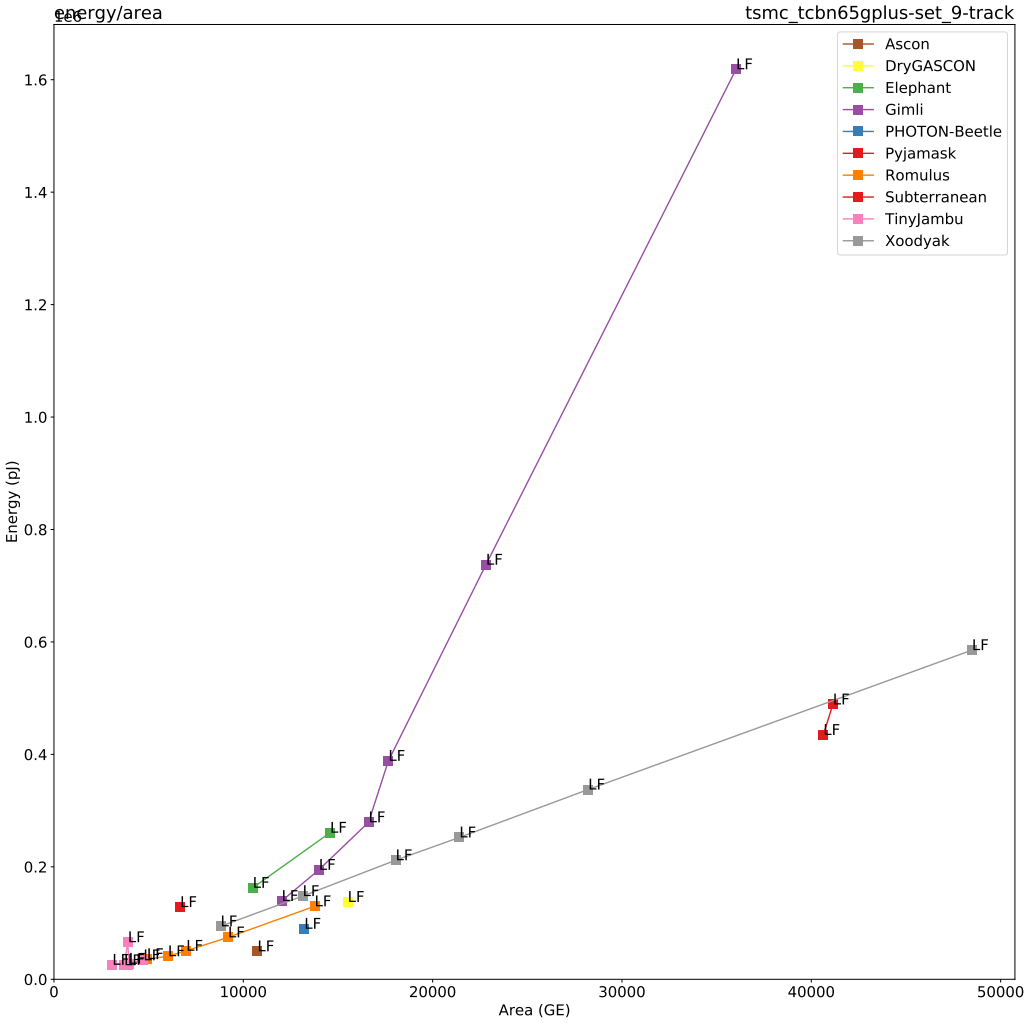

Figure 73: 3 Mbps: Energy vs. Area for $|M| = 64$ bytes on TSMC 65nm.

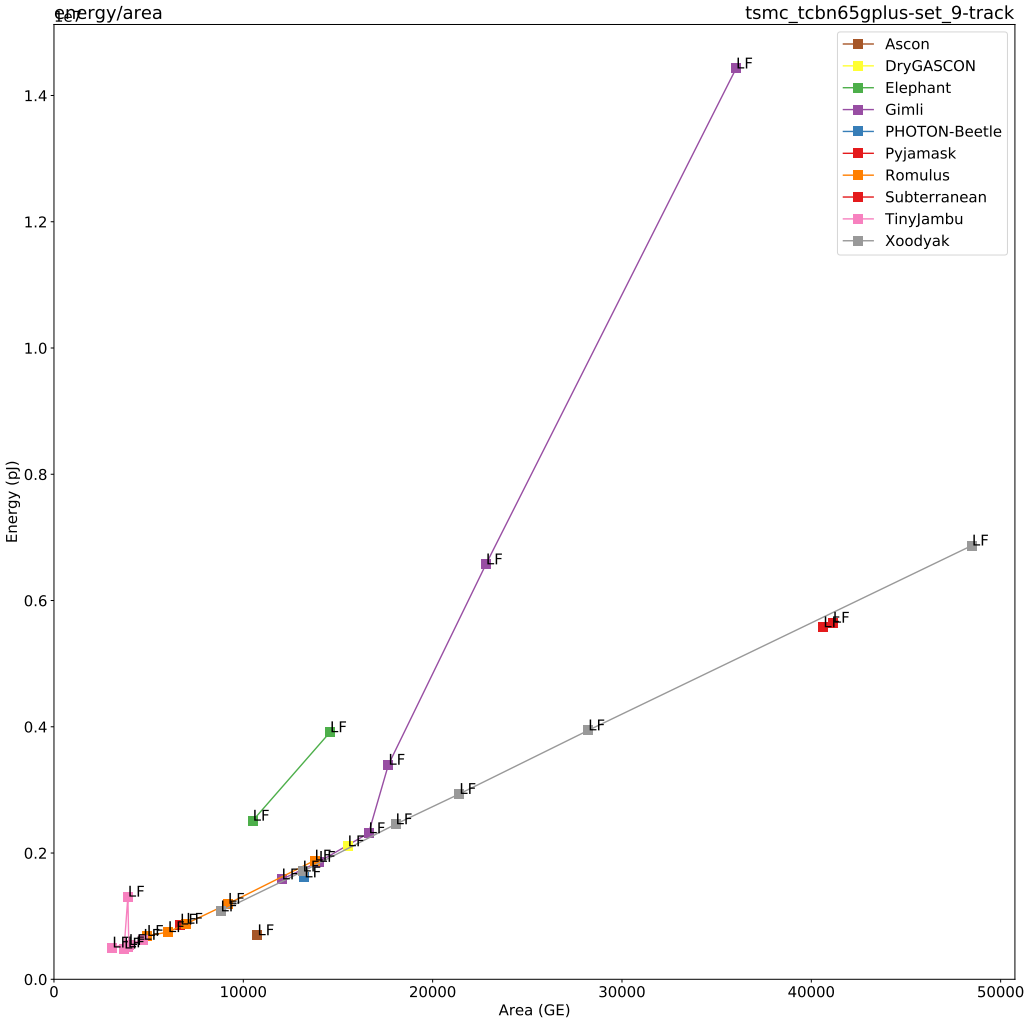

Figure 74: 3 Mbps: Energy vs. Area for |M| = 1536 bytes on TSMC 65nm.

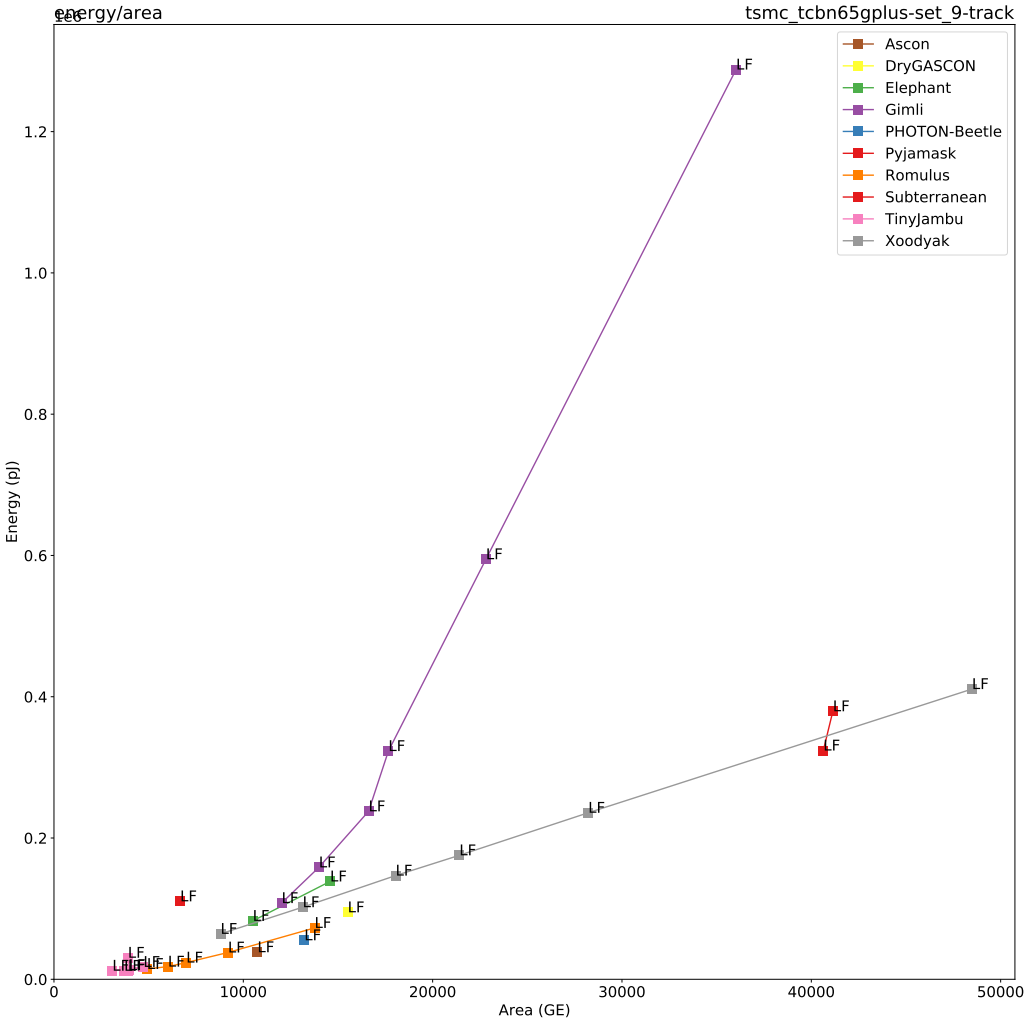

Figure 75: 3 Mbps: Energy vs. Area for $|A| = |M| = 16$ bytes on TSMC 65nm.

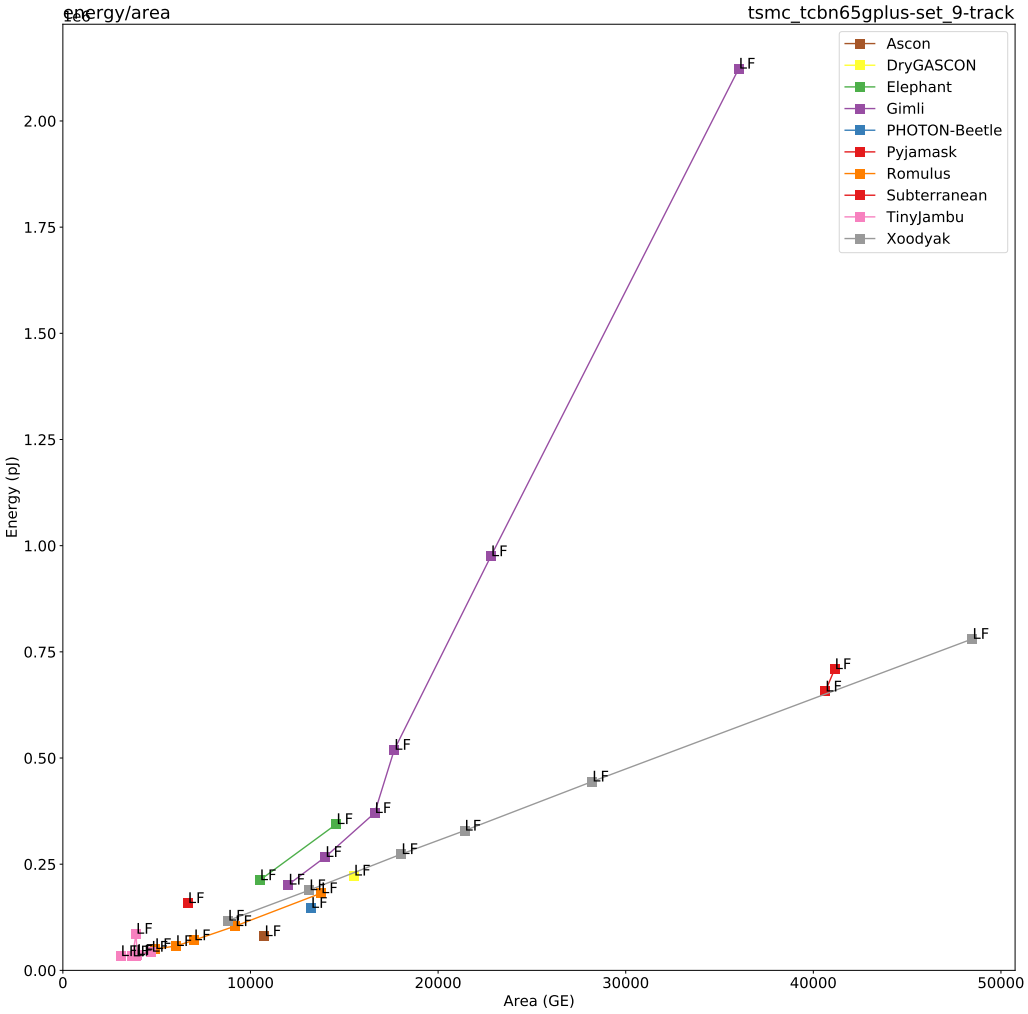

Figure 76: 3 Mbps: Energy vs. Area for $|A| = |M| = 64$ bytes on TSMC 65nm.

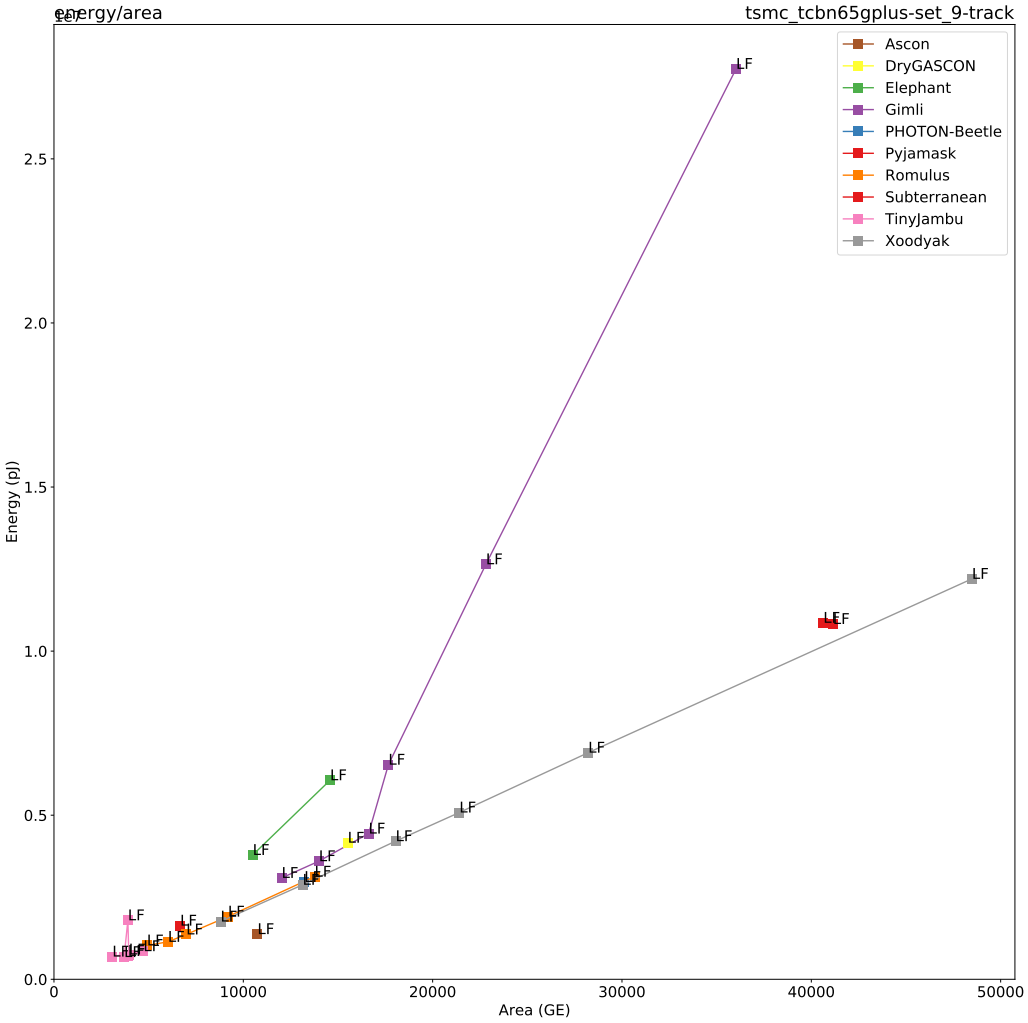

Figure 77: 3 Mbps: Energy vs. Area for $|A| = |M| = 1536$ bytes on TSMC 65nm.

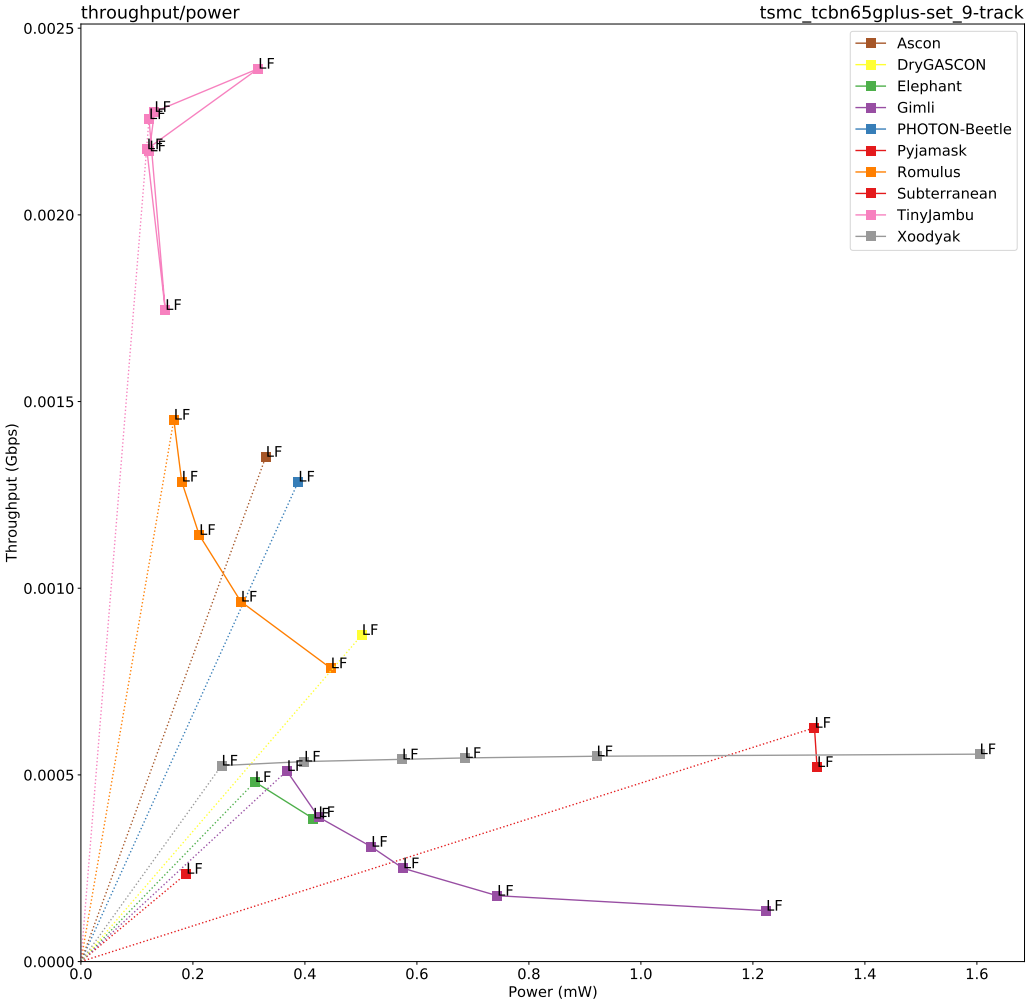

Figure 78: 3 Mbps: Throughput vs. Power for |A| = 16 bytes on TSMC 65nm.

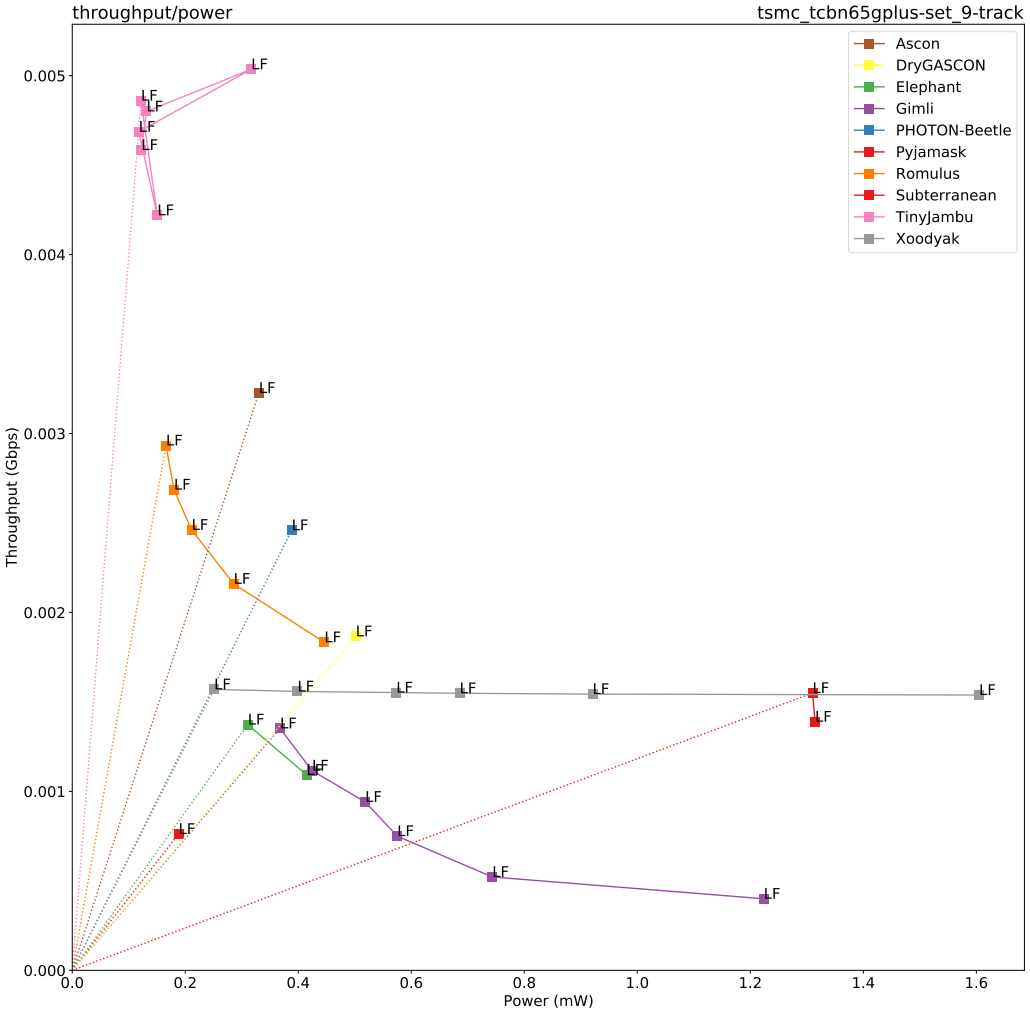

Figure 79: 3 Mbps: Throughput vs. Power for |A| = 64 bytes on TSMC 65nm.

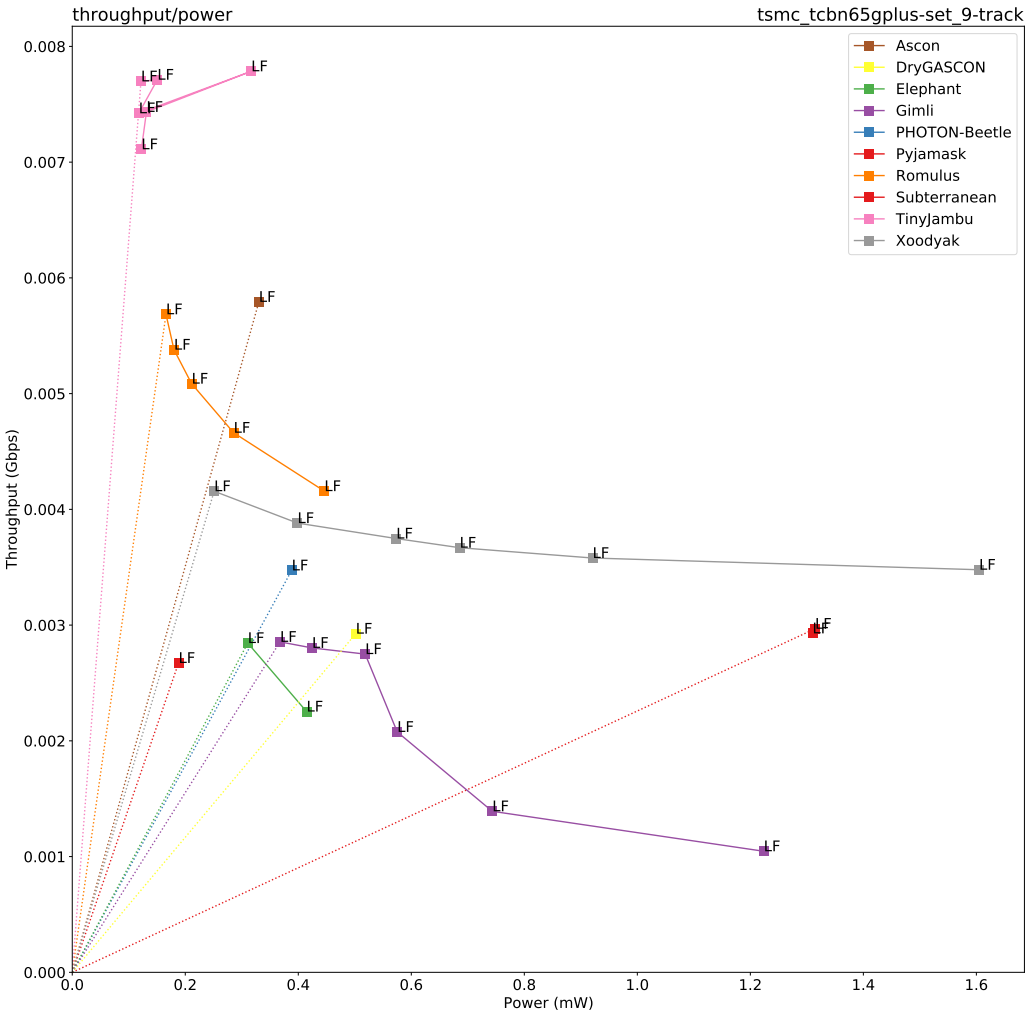

Figure 80: 3 Mbps: Throughput vs. Power for |A| = 1536 bytes on TSMC 65nm.

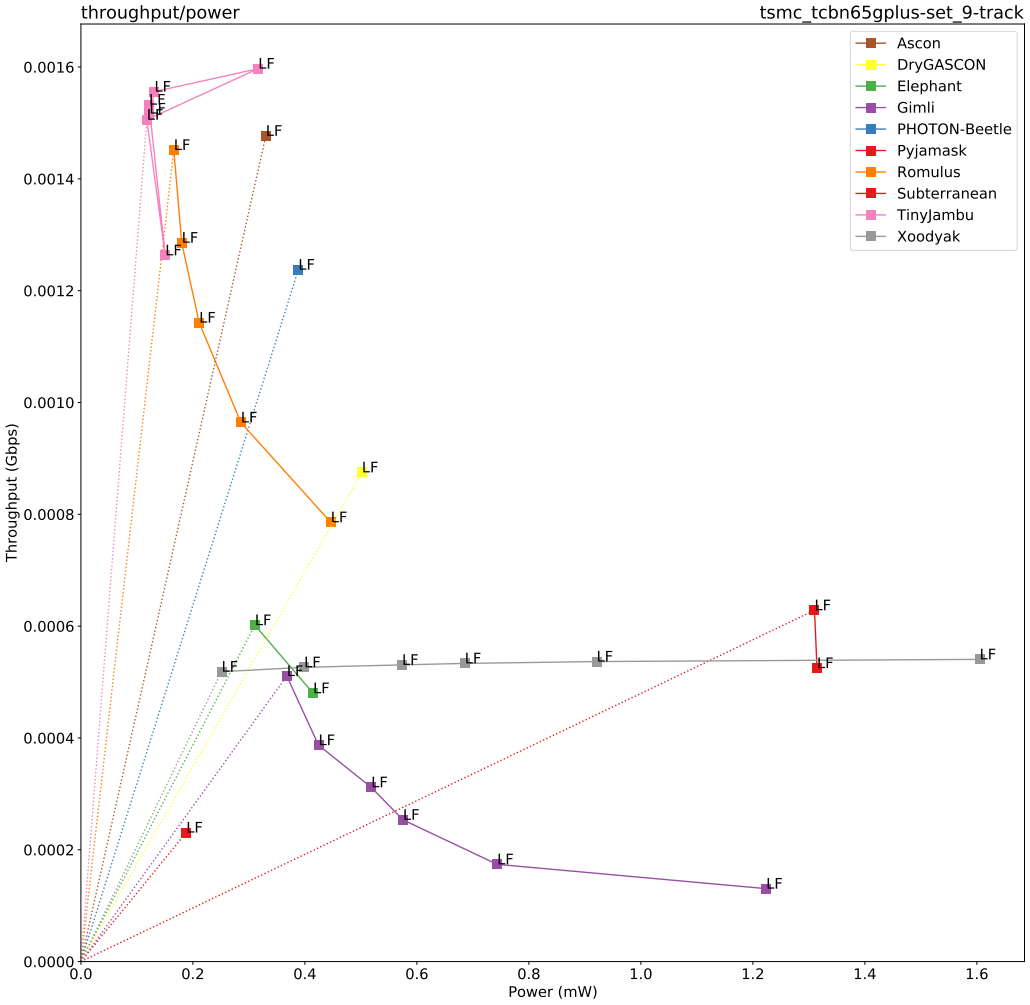

Figure 81: 3 Mbps: Throughput vs. Power for |M| = 16 bytes on TSMC 65nm.

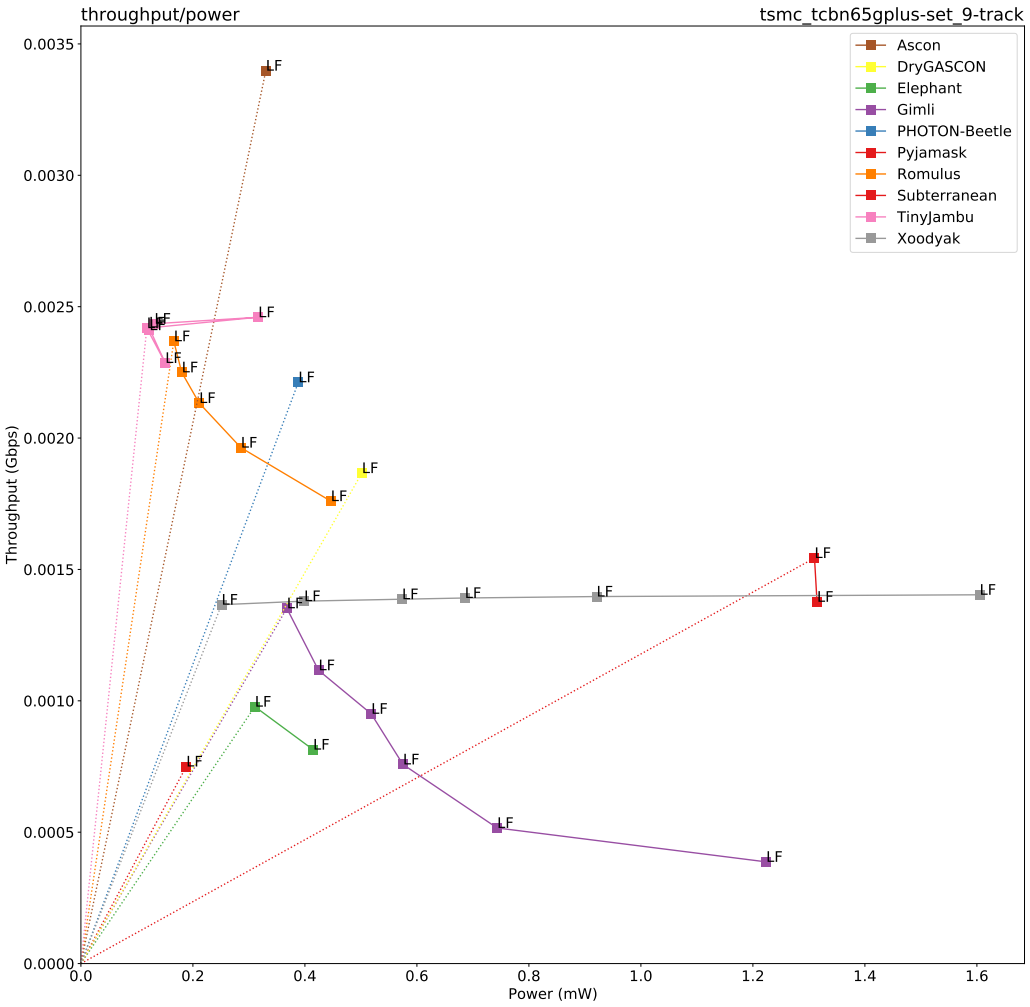

Figure 82: 3 Mbps: Throughput vs. Power for |M| = 64 bytes on TSMC 65nm.

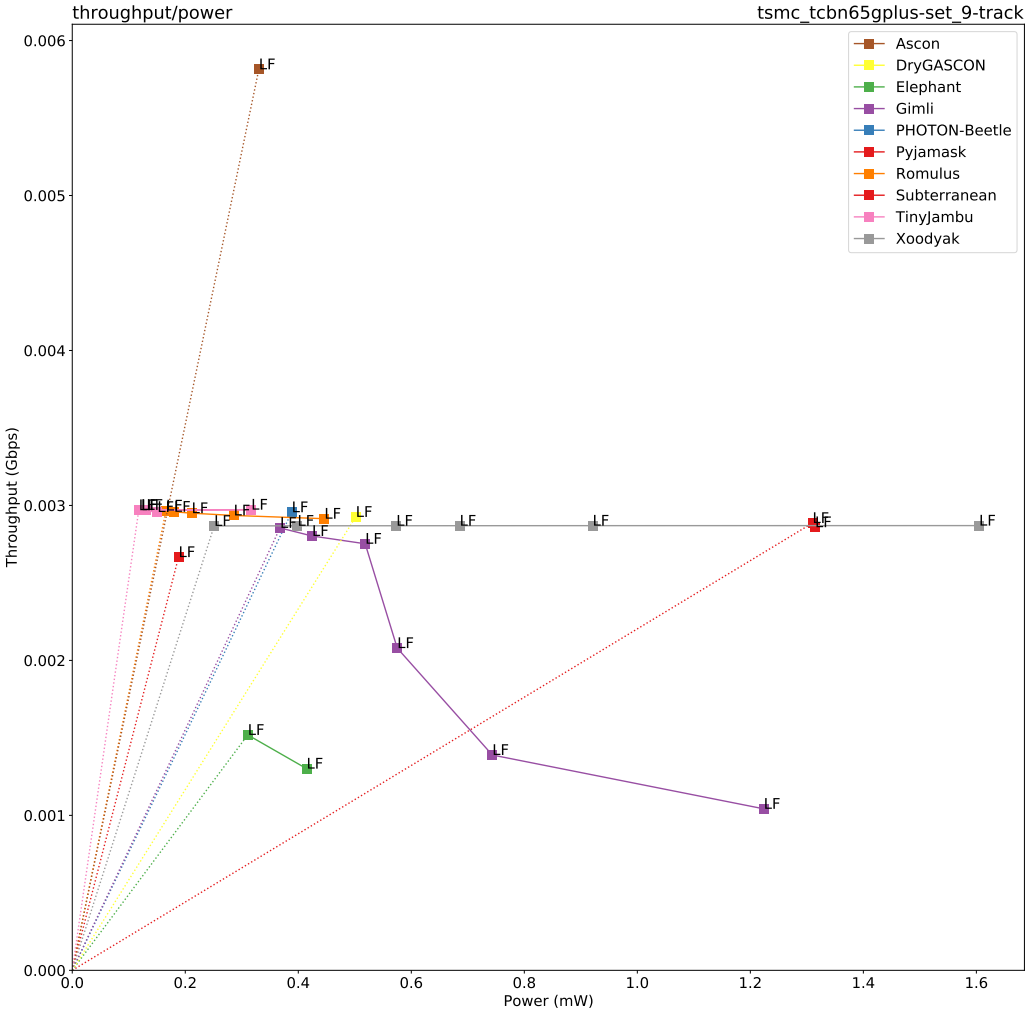

Figure 83: 3 Mbps: Throughput vs. Power for |M| = 1536 bytes on TSMC 65nm.

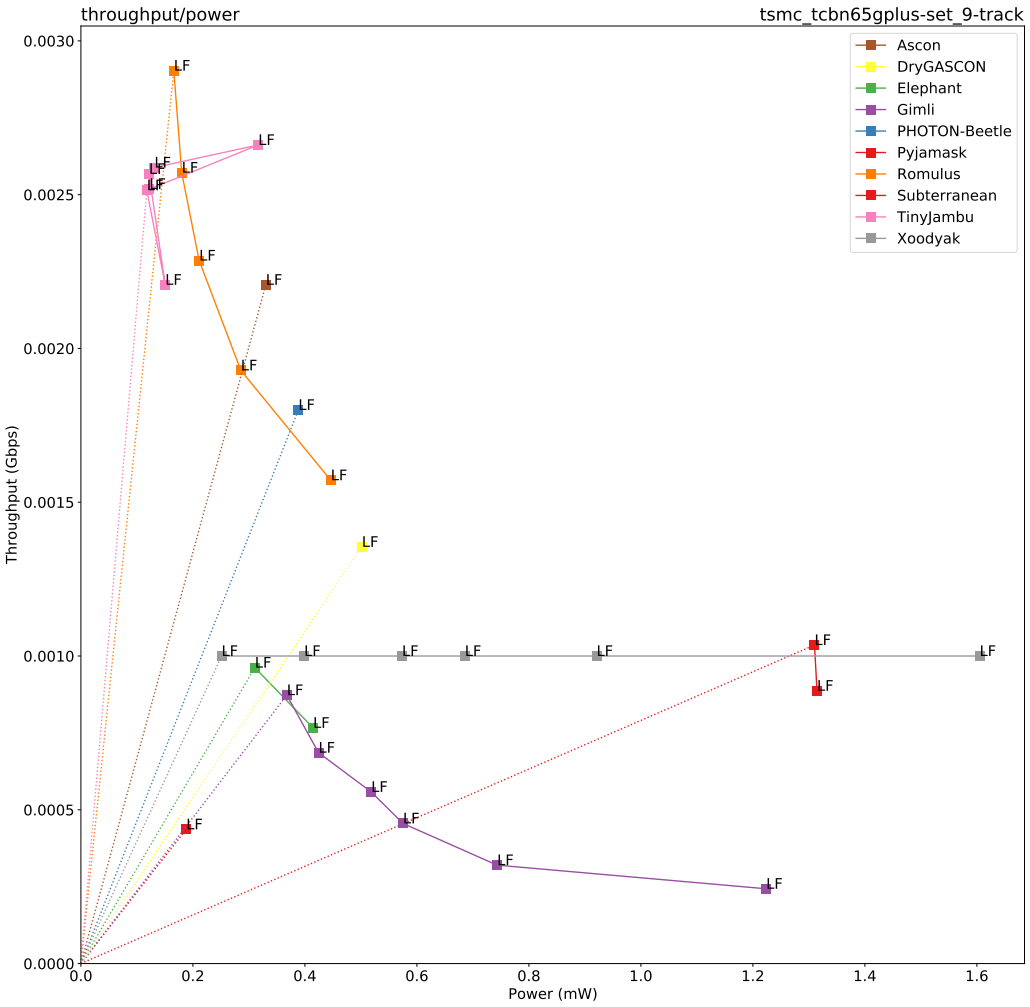

Figure 84: 3 Mbps: Throughput vs. Power for |A| = |M| = 16 bytes on TSMC 65nm.

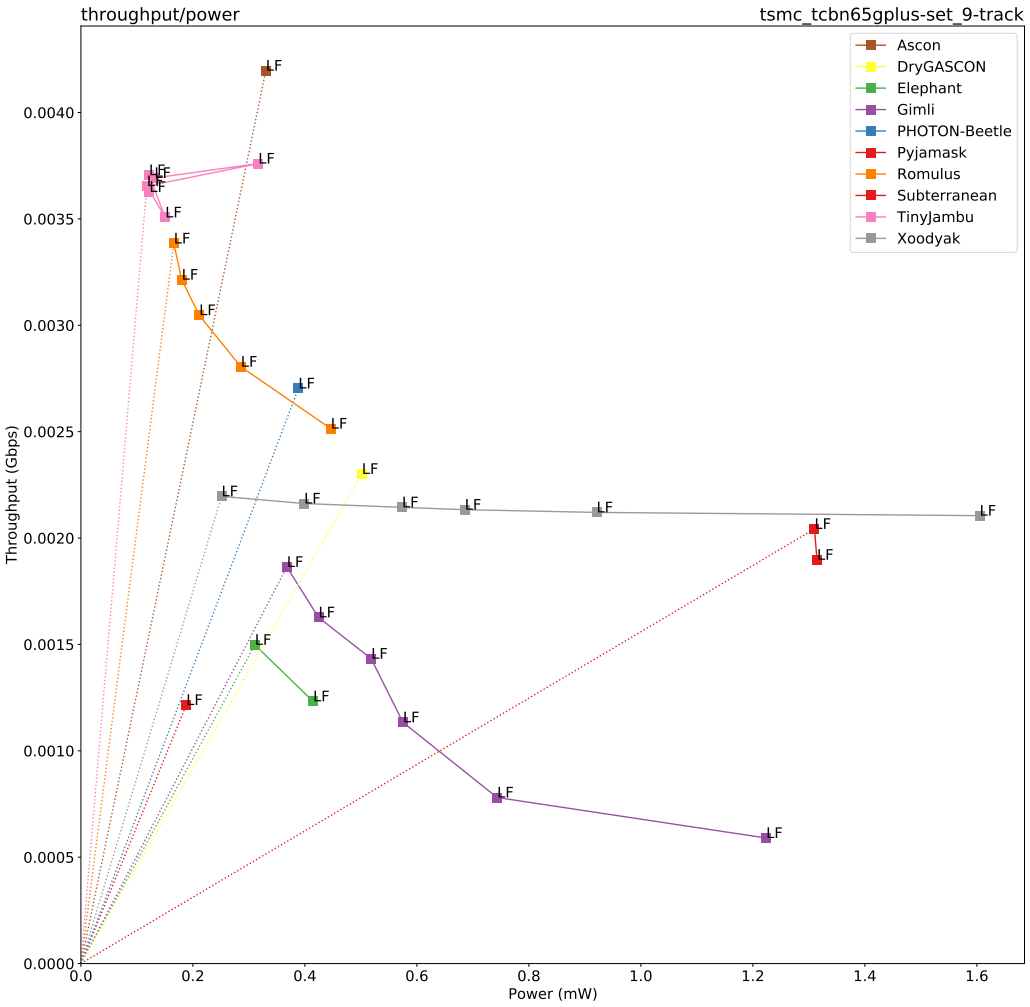

Figure 85: 3 Mbps: Throughput vs. Power for |A| = |M| = 64 bytes on TSMC 65nm.

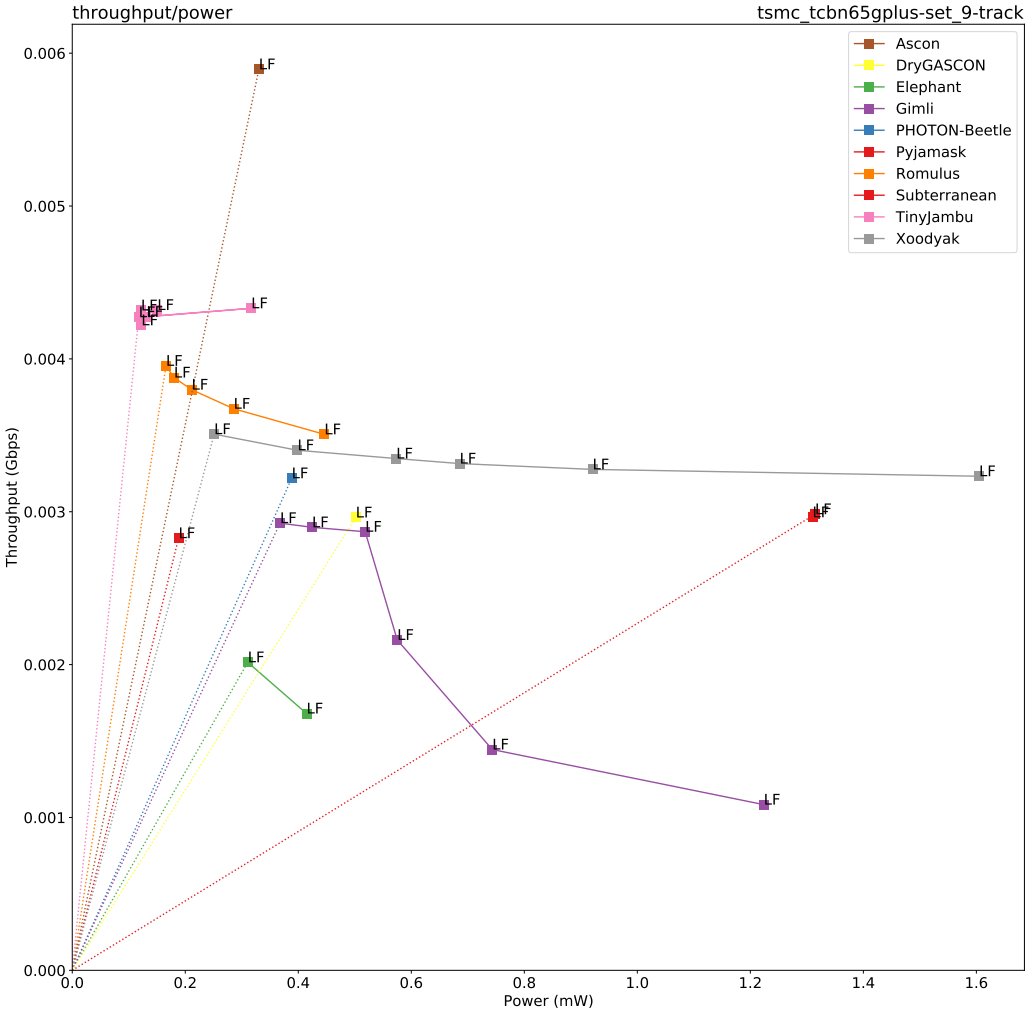

Figure 86: 3 Mbps: Throughput vs. Power for |A| = |M| = 1536 bytes on TSMC 65nm.

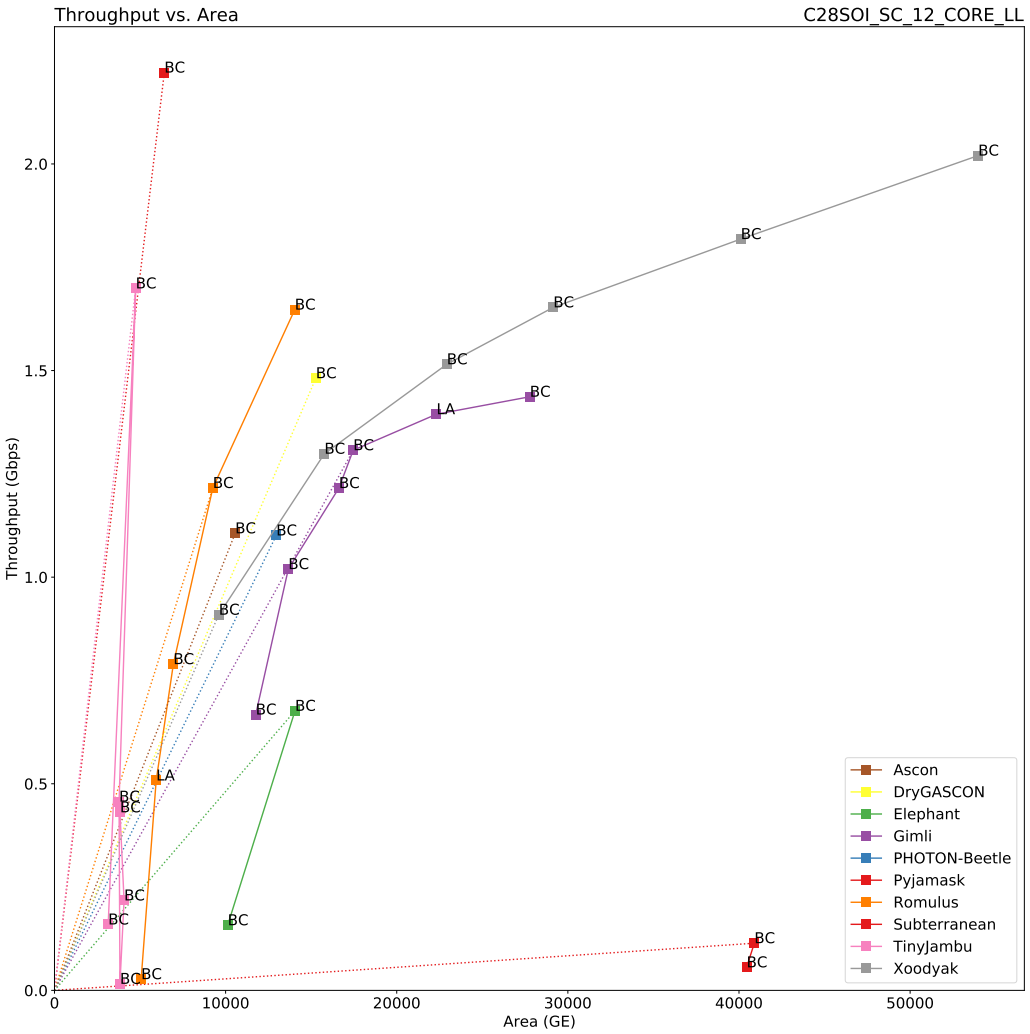

Figure 87: Throughput vs. Area for $|A| = 16$ bytes on FDSOI 28nm.

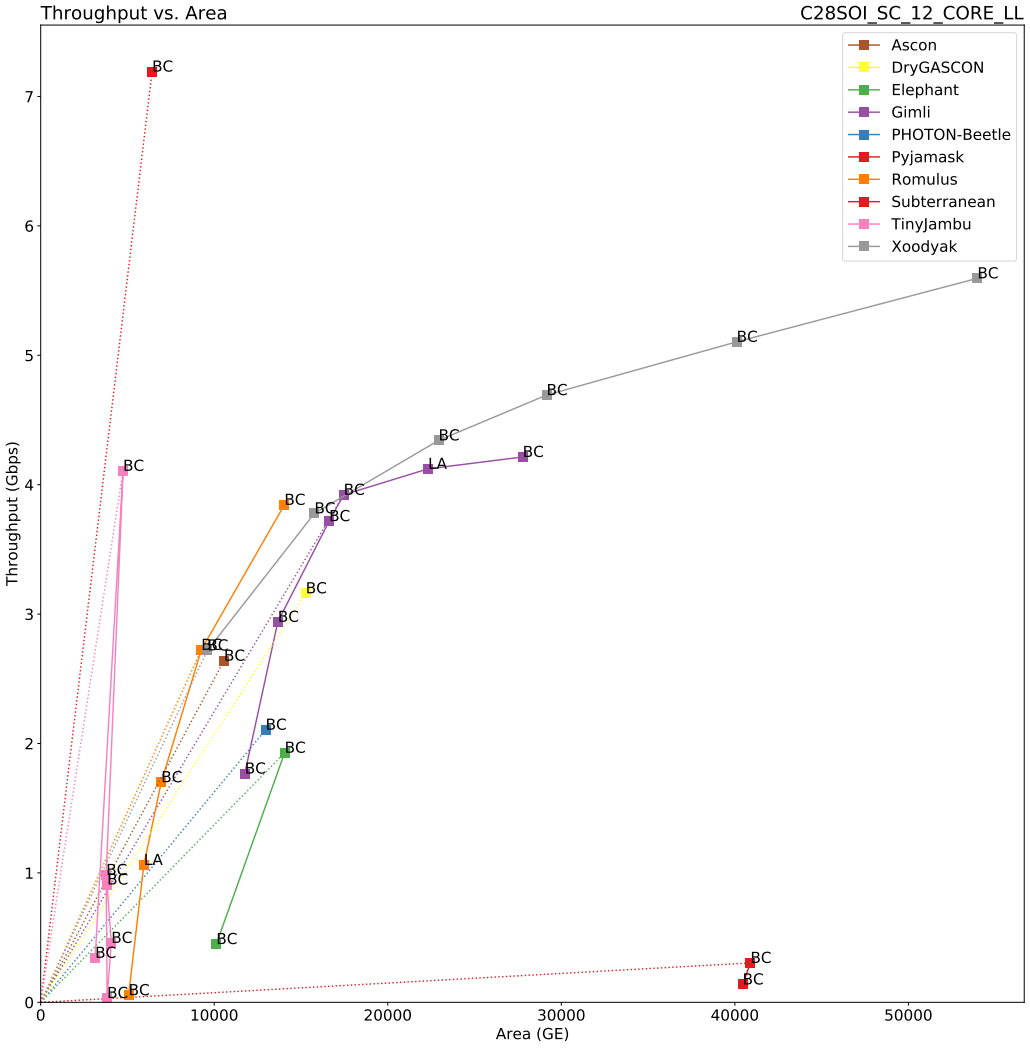

Figure 88: Throughput vs. Area for |A| = 64 bytes on FDSOI 28nm.

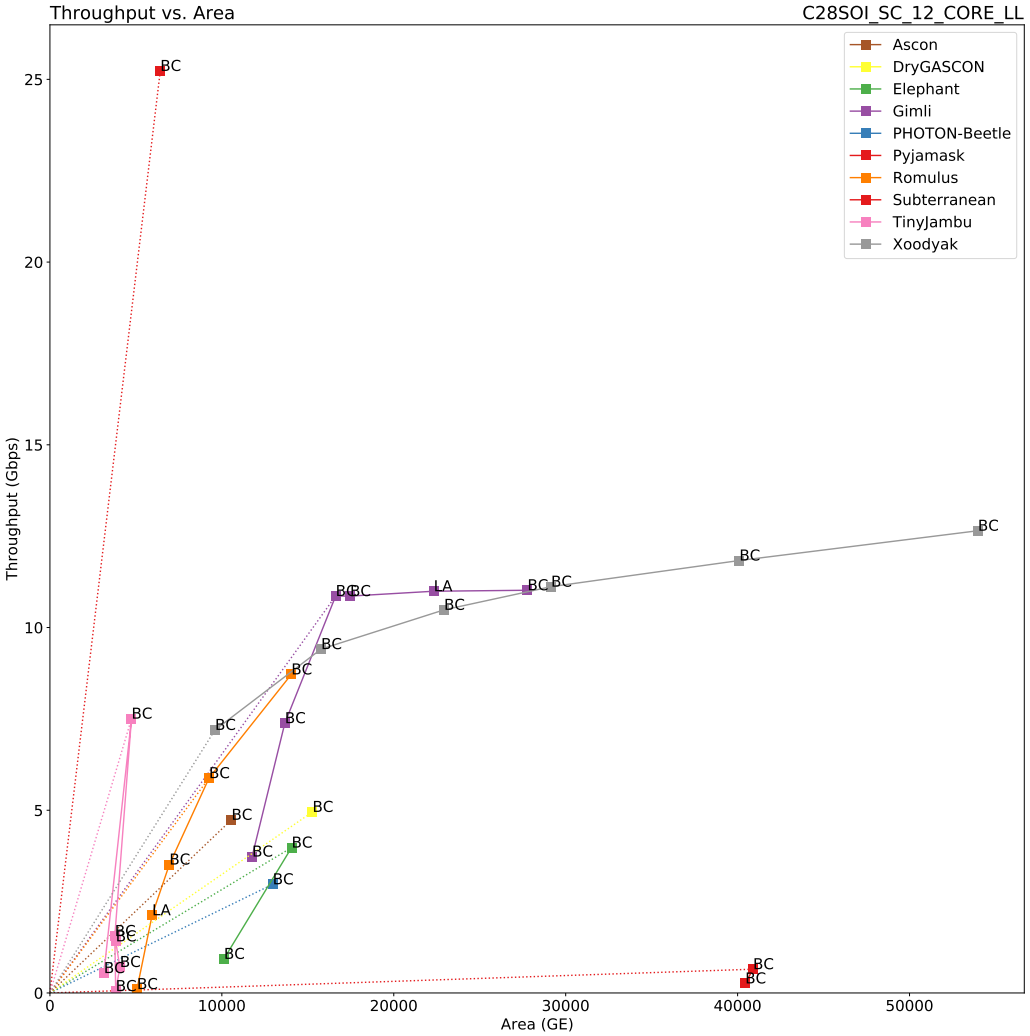

Figure 89: Throughput vs. Area for $|A| = 1536$ bytes on FDSOI 28nm.

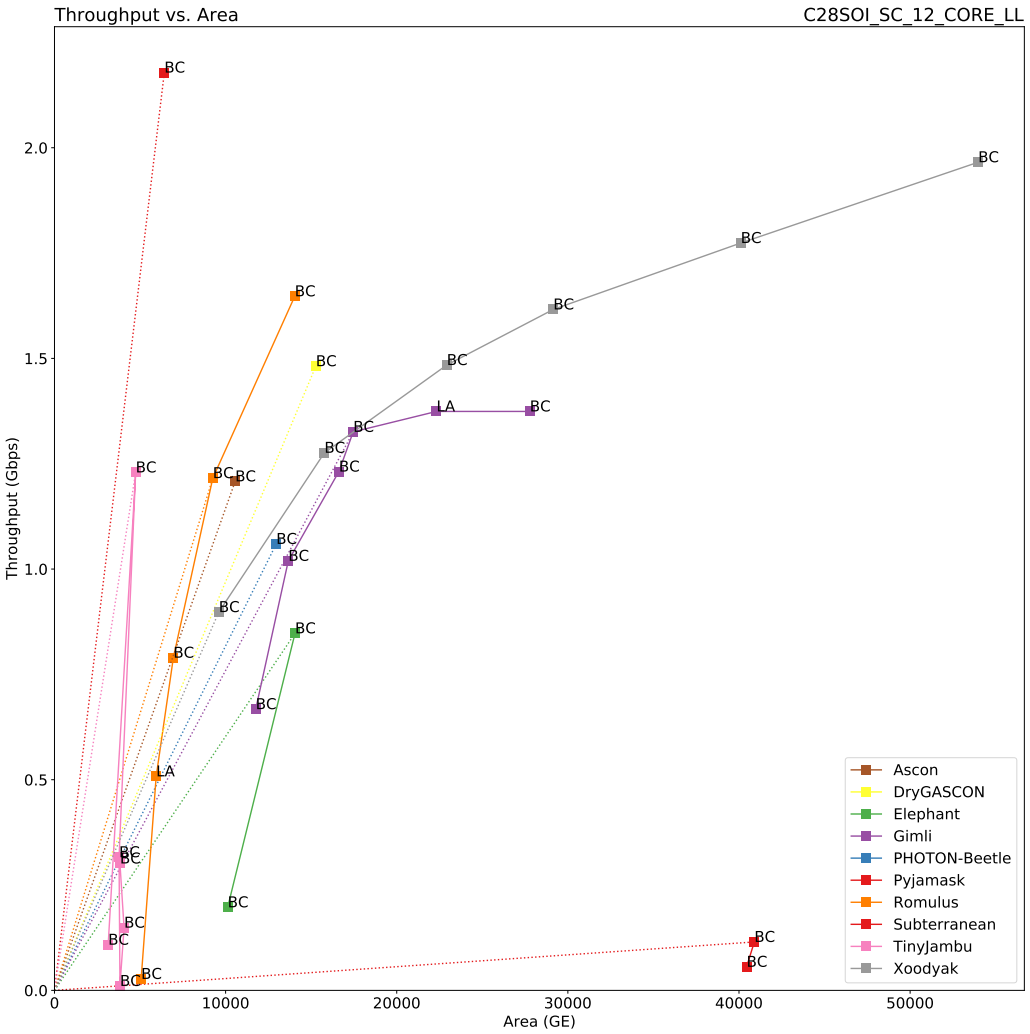

Figure 90: Throughput vs. Area for |M| = 16 bytes on FDSOI 28nm.

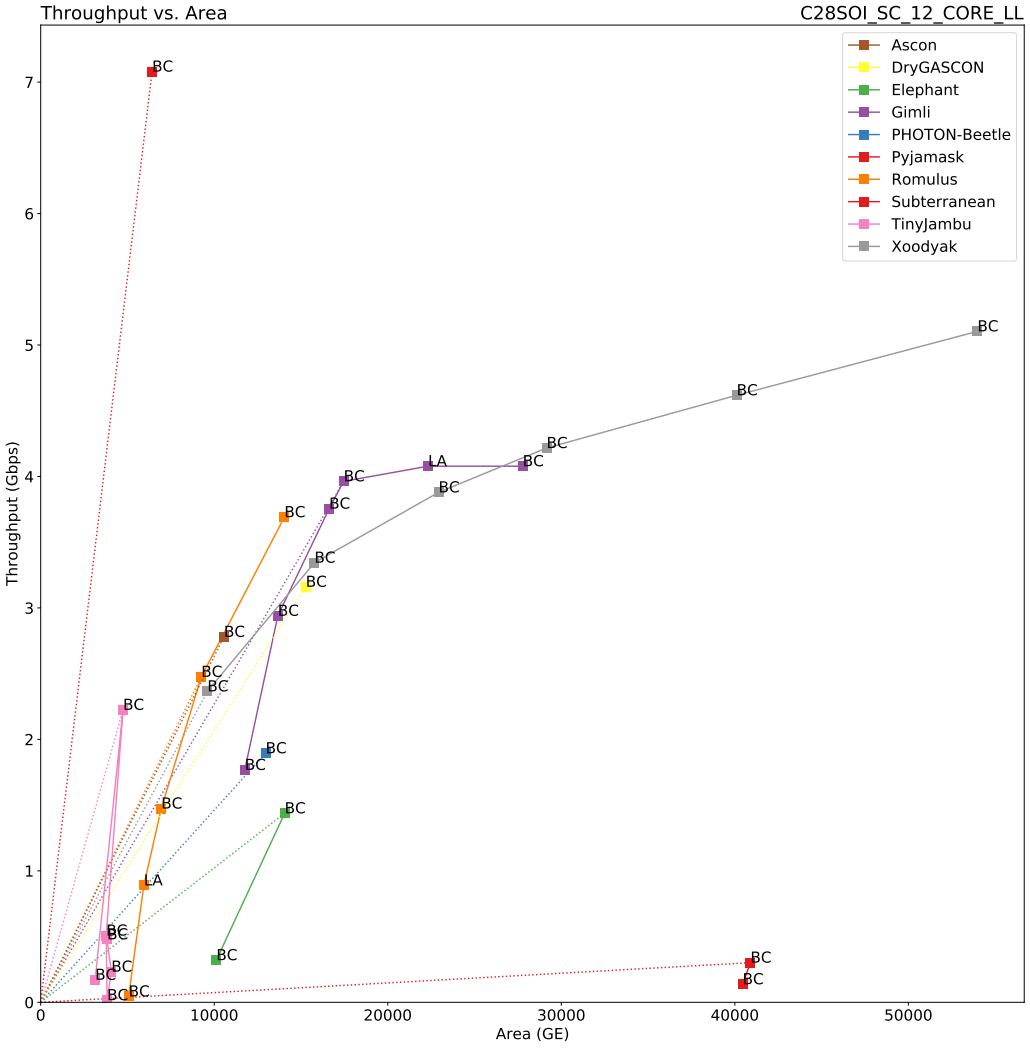

Figure 91: Throughput vs. Area for |M| = 64 bytes on FDSOI 28nm.

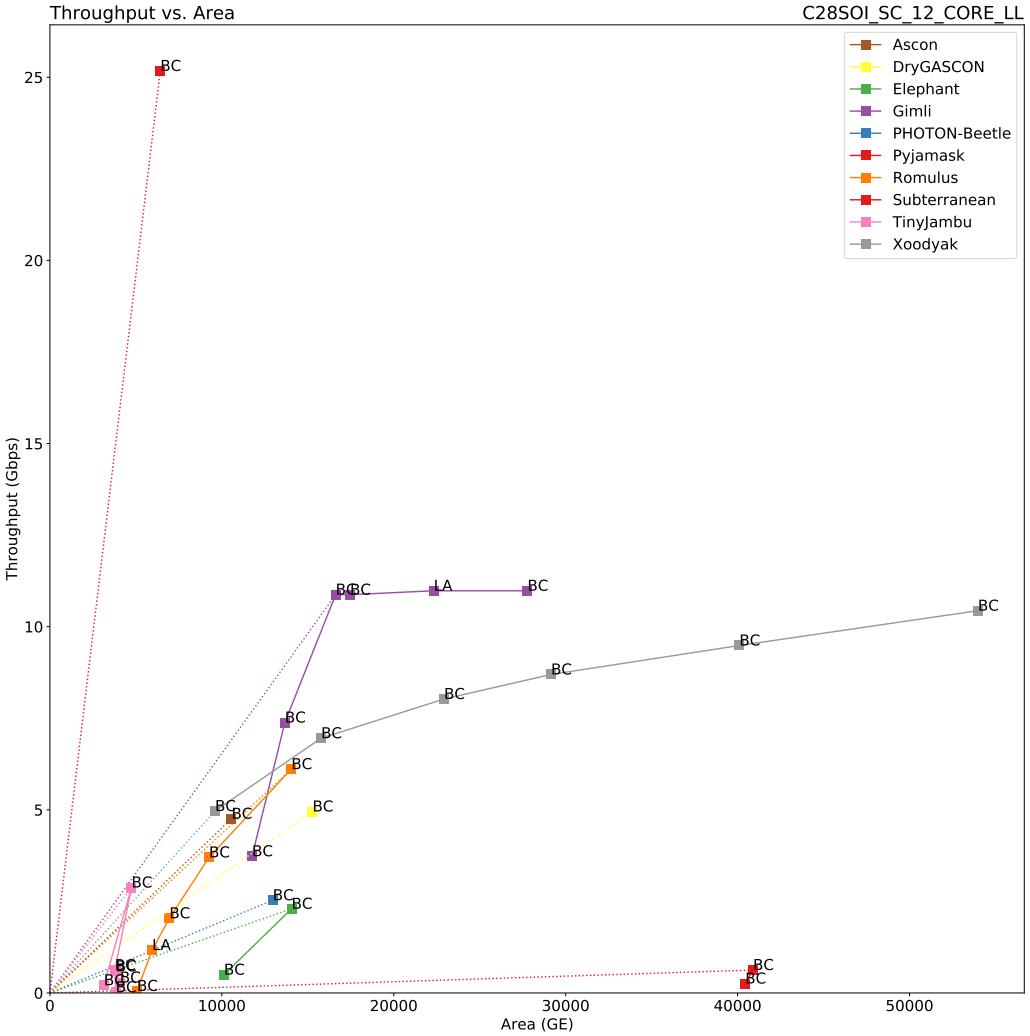

Figure 92: Throughput vs. Area for |M| = 1536 bytes on FDSOI 28nm.

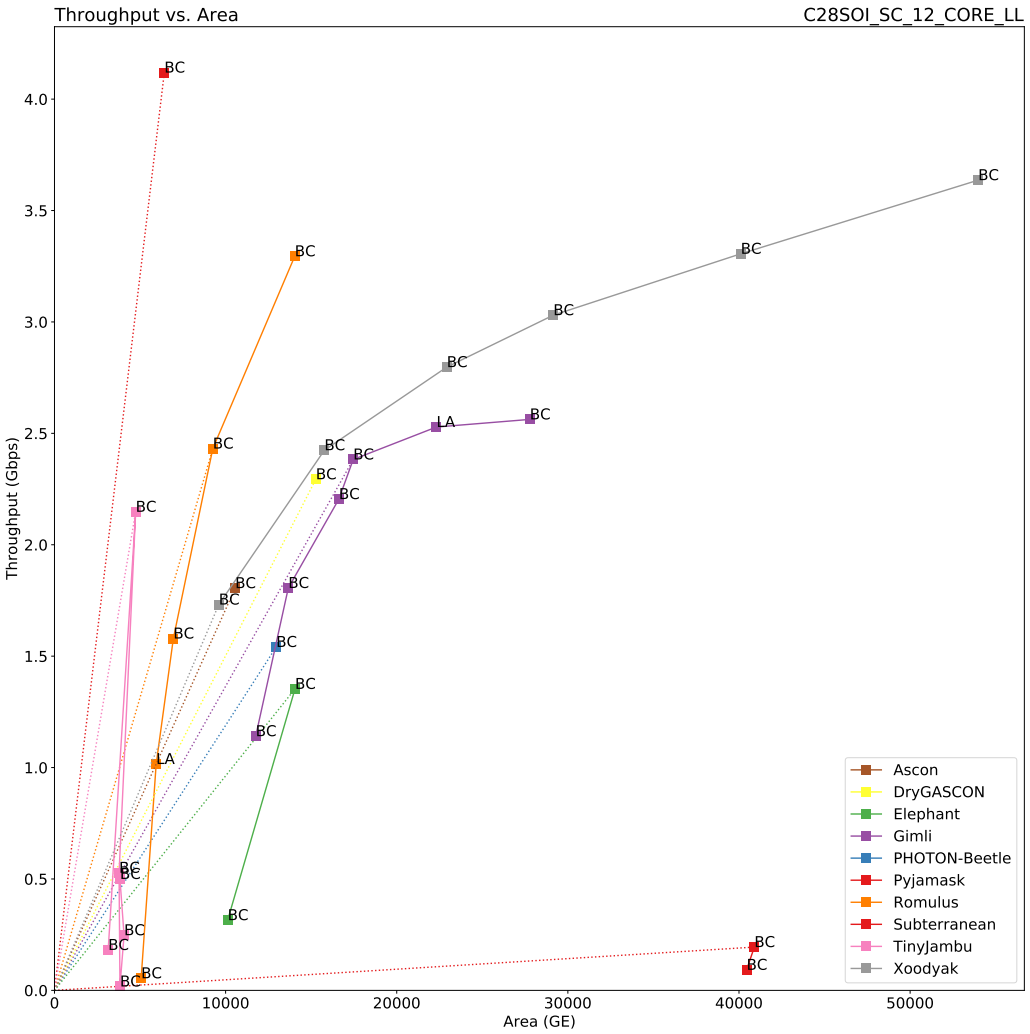

Figure 93: Throughput vs. Area for |A| = |M| = 16 bytes on FDSOI 28nm.

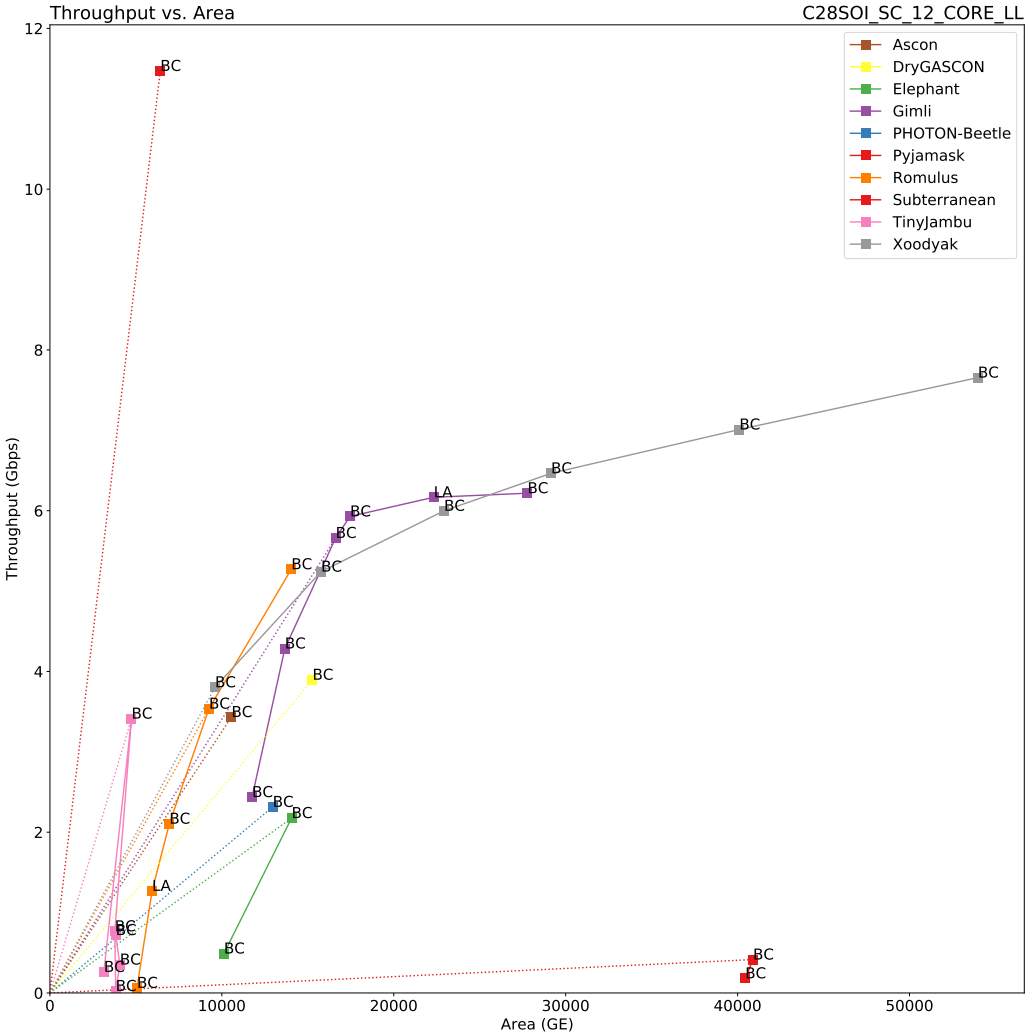

Figure 94: Throughput vs. Area for |A| = |M| = 64 bytes on FDSOI 28nm.

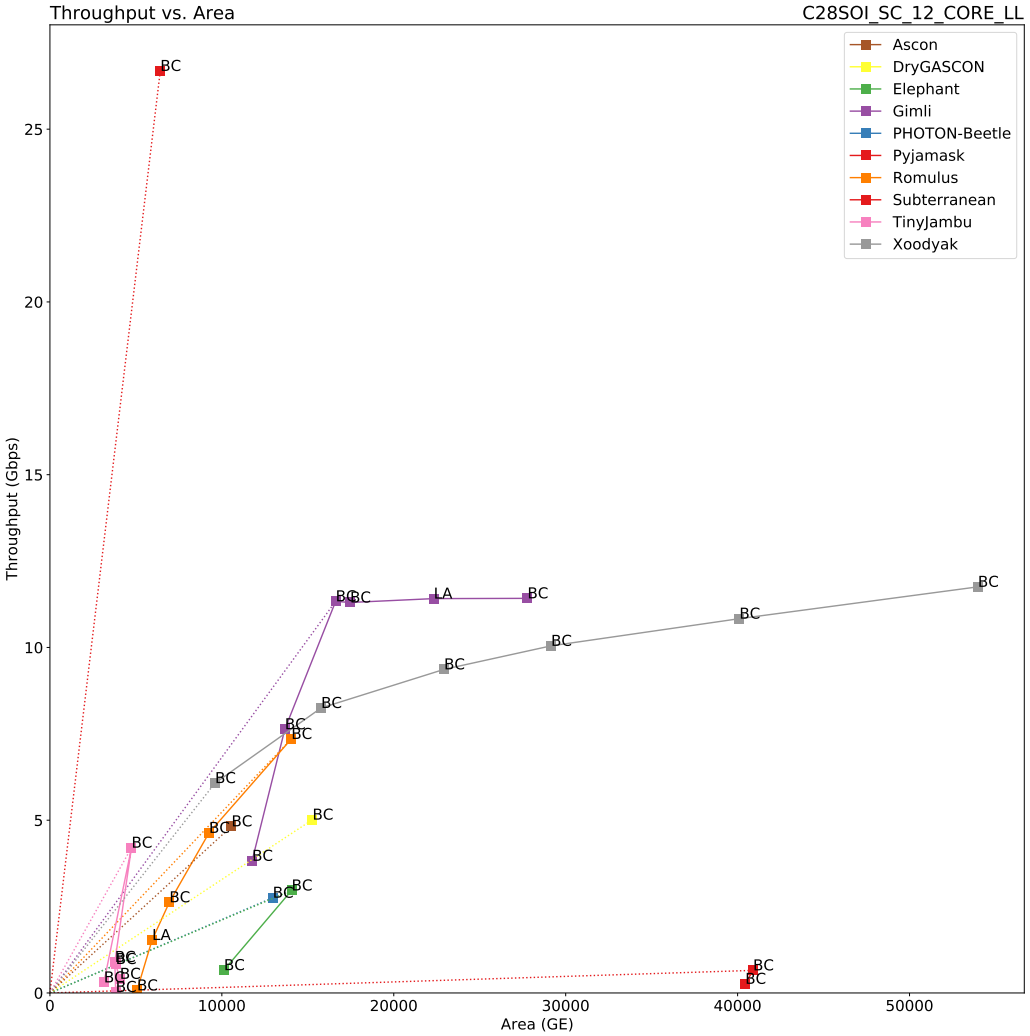

Figure 95: Throughput vs. Area for $|A| = |M| = 1536$ bytes on FDSOI 28nm.

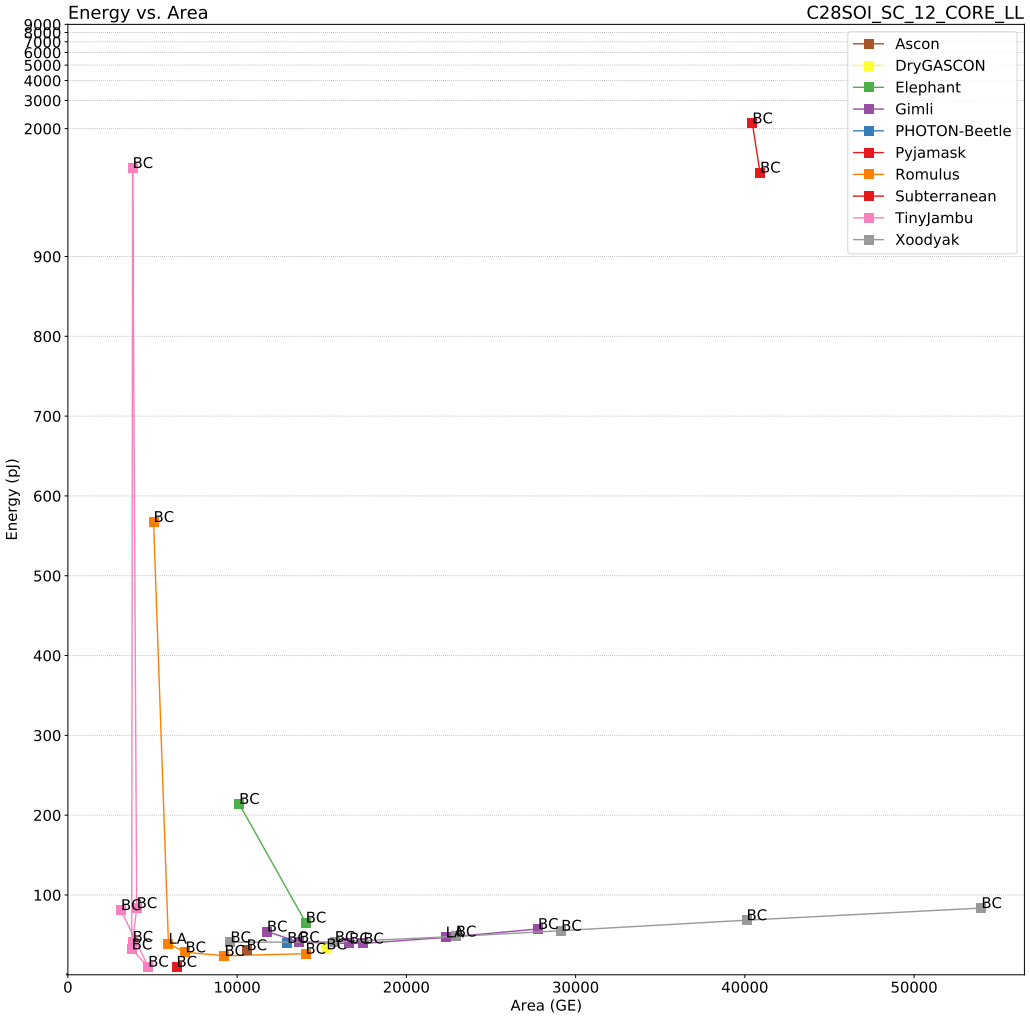

Figure 96: Energy vs. Area for $|A| = 16$ bytes on FDSOI 28nm. The energy axis follows a log scale for values $\geqslant 900$ pJ on FDSOI 28nm.

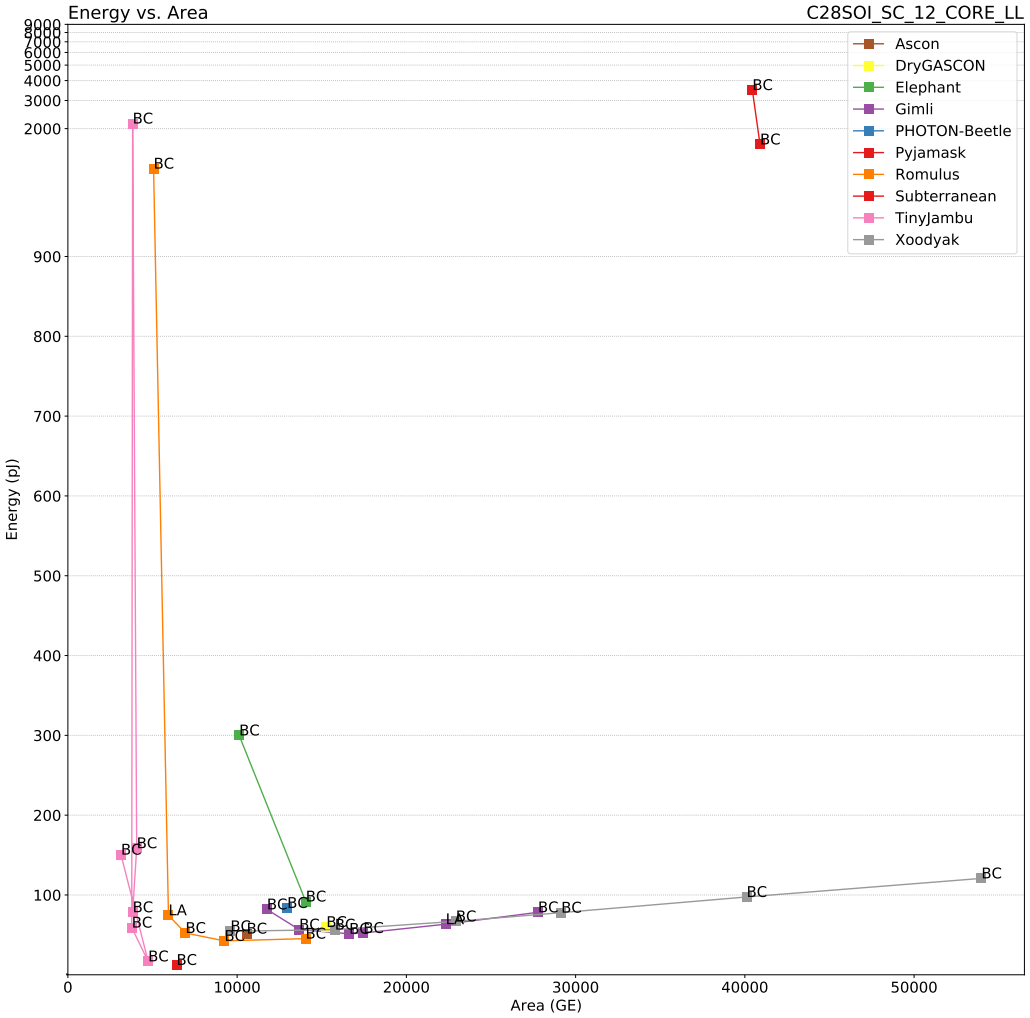

Figure 97: Energy vs. Area for $|A| = 64$ bytes on FDSOI 28nm. The energy axis follows a log scale for values $\geqslant 900$ pJ on FDSOI 28nm.

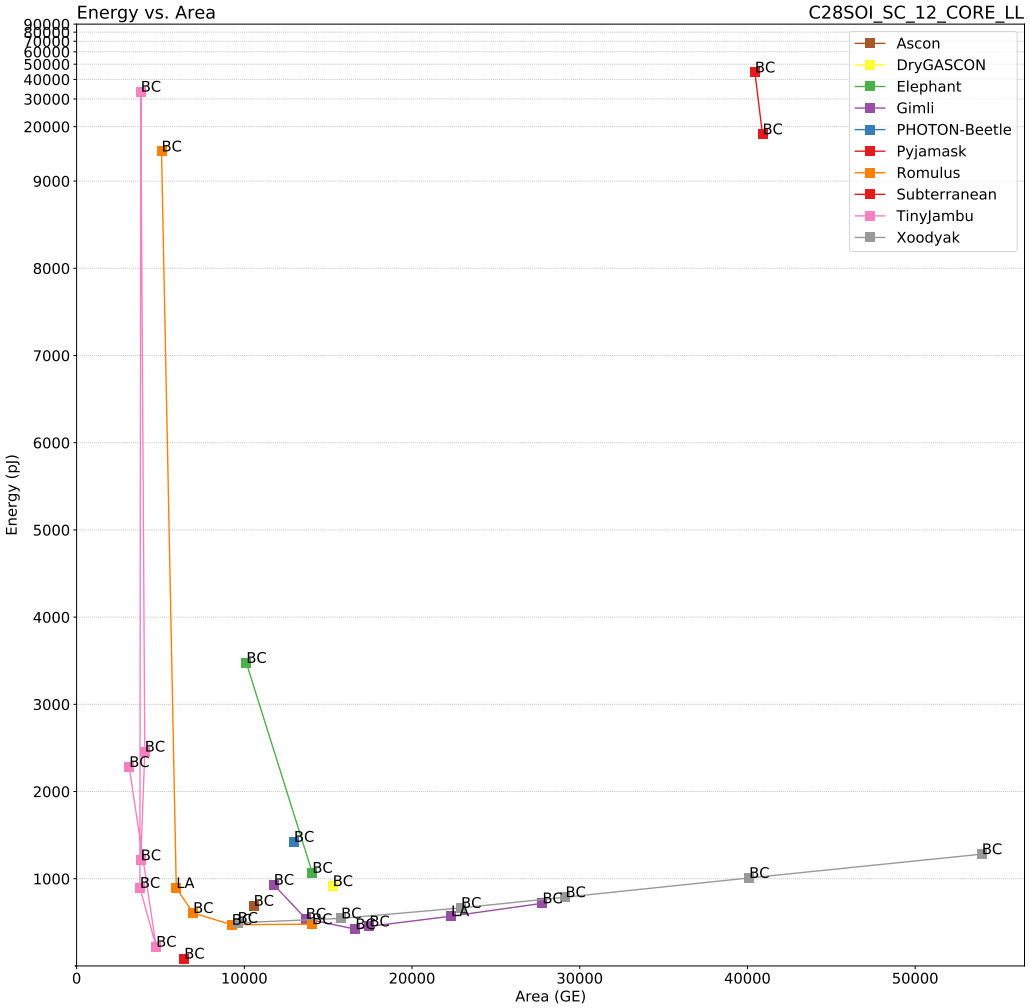

Figure 98: Energy vs. Area for $|A| = 1536$ bytes. The energy axis follows a log scale for values $\geqslant 9000$ pJ on FDSOI 28nm.

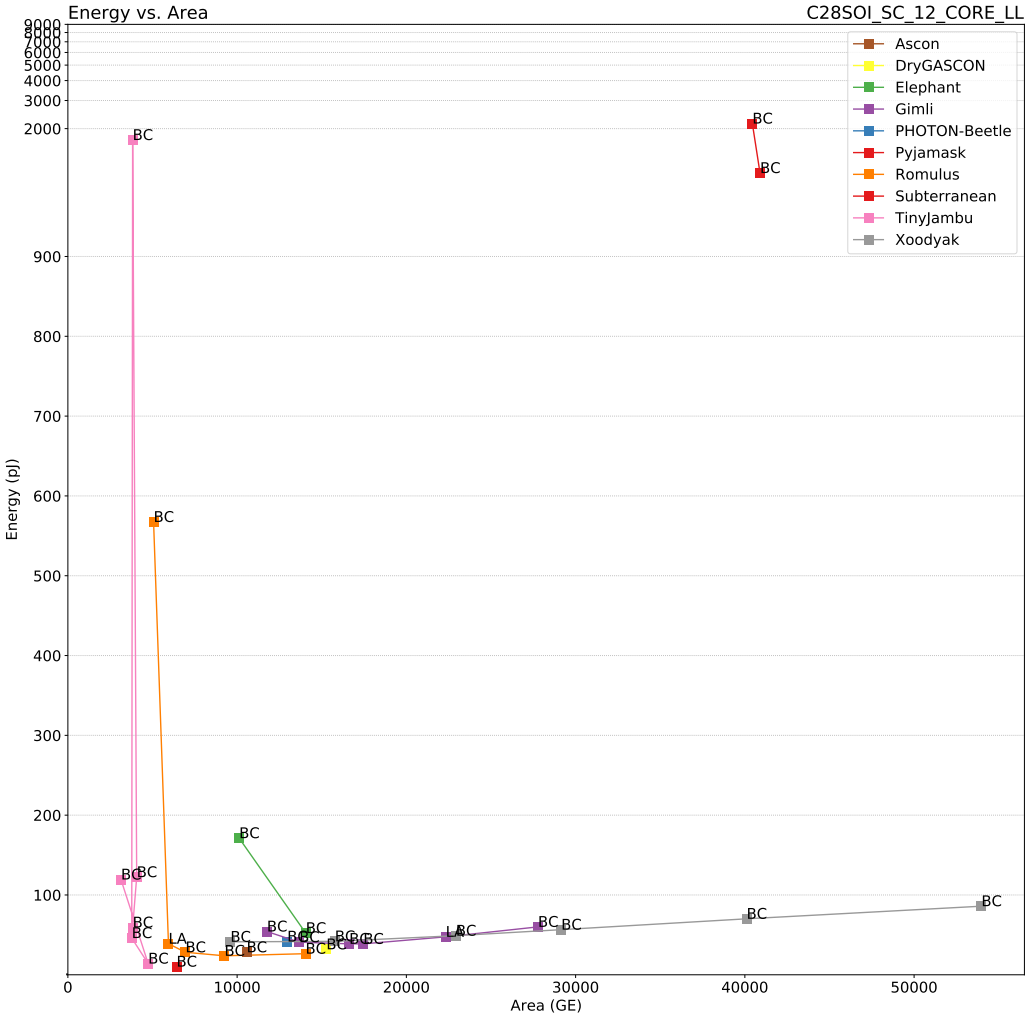

Figure 99: Energy vs. Area for $|M| = 16$ bytes on FDSOI 28nm. The energy axis follows a log scale for values $\geqslant 900$ pJ.

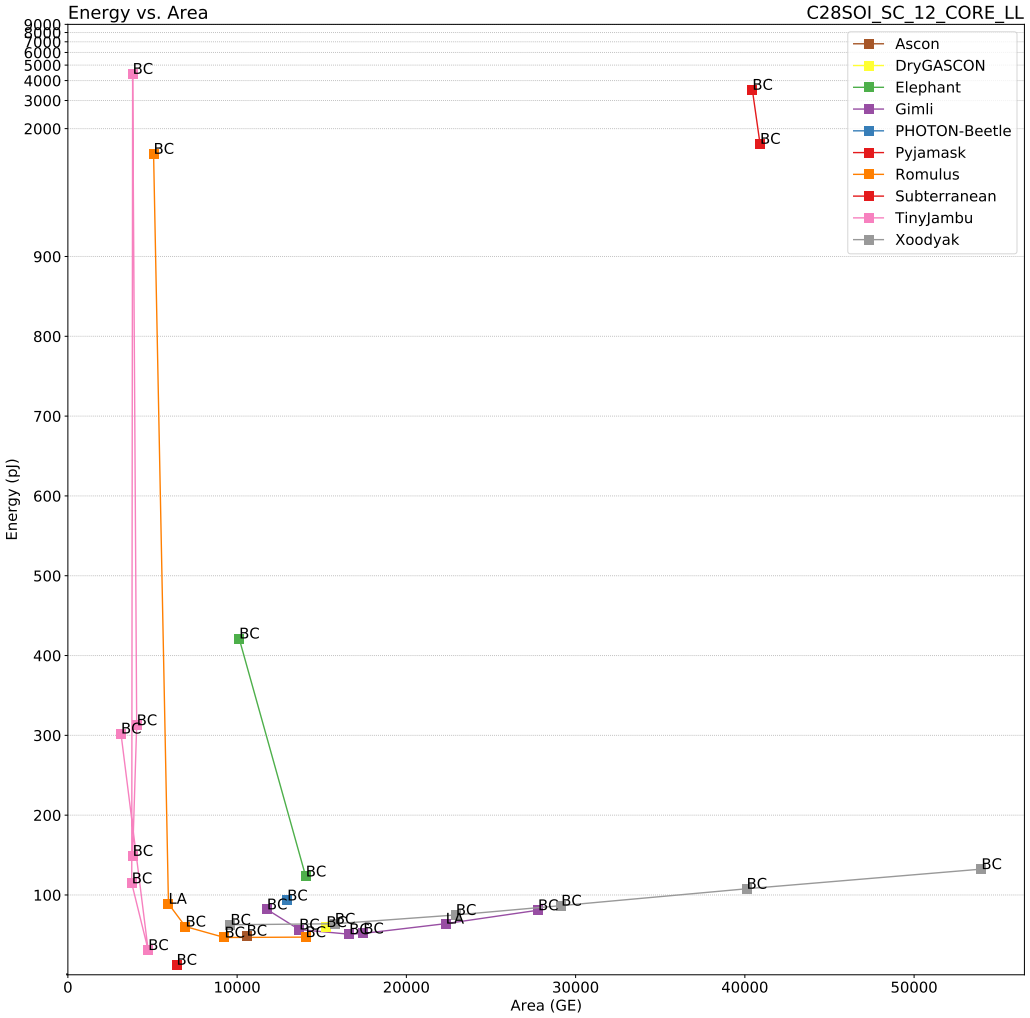

Figure 100: Energy vs. Area for $|M| = 64$ bytes on FDSOI 28nm. The energy axis follows a log scale for values $\geqslant 900$ pJ.

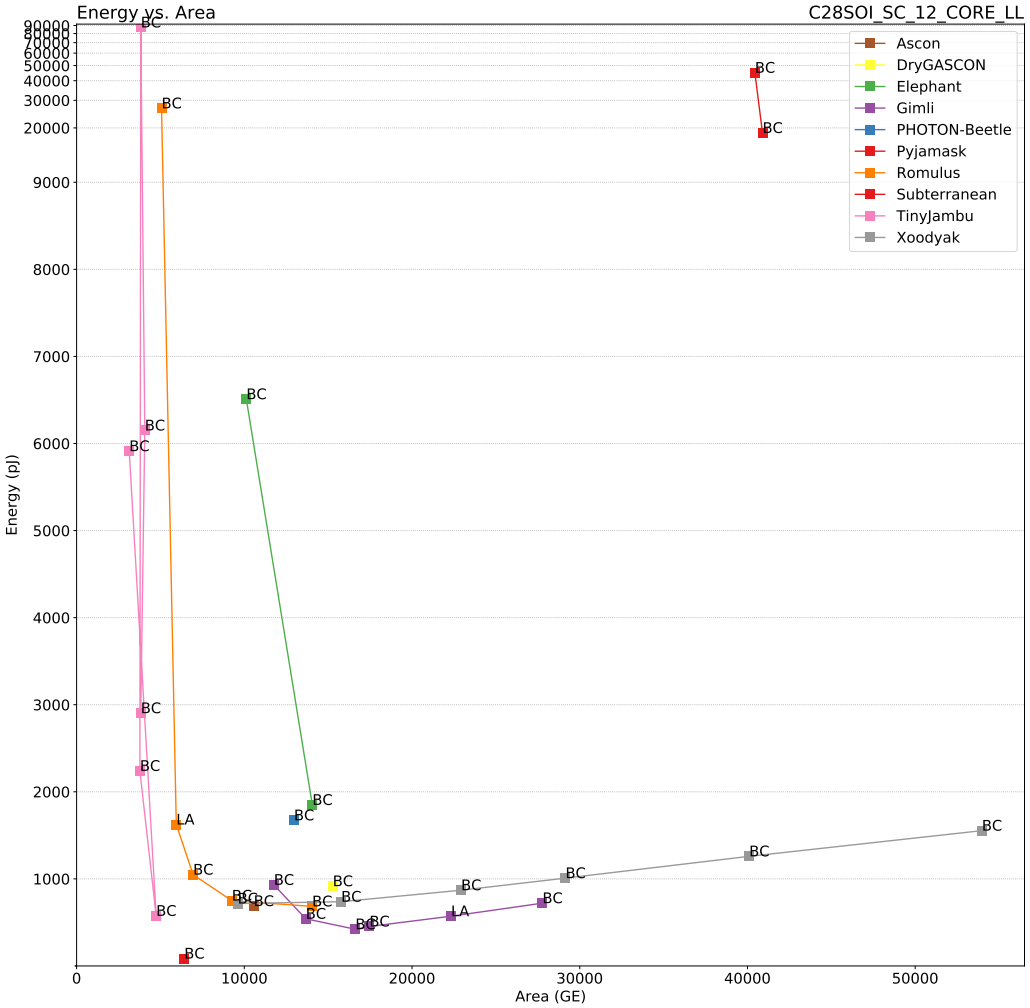

Figure 101: Energy vs. Area for $|M| = 1536$ bytes on FDSOI 28nm. The energy axis follows a log scale for values $\geqslant 9000$ pJ.

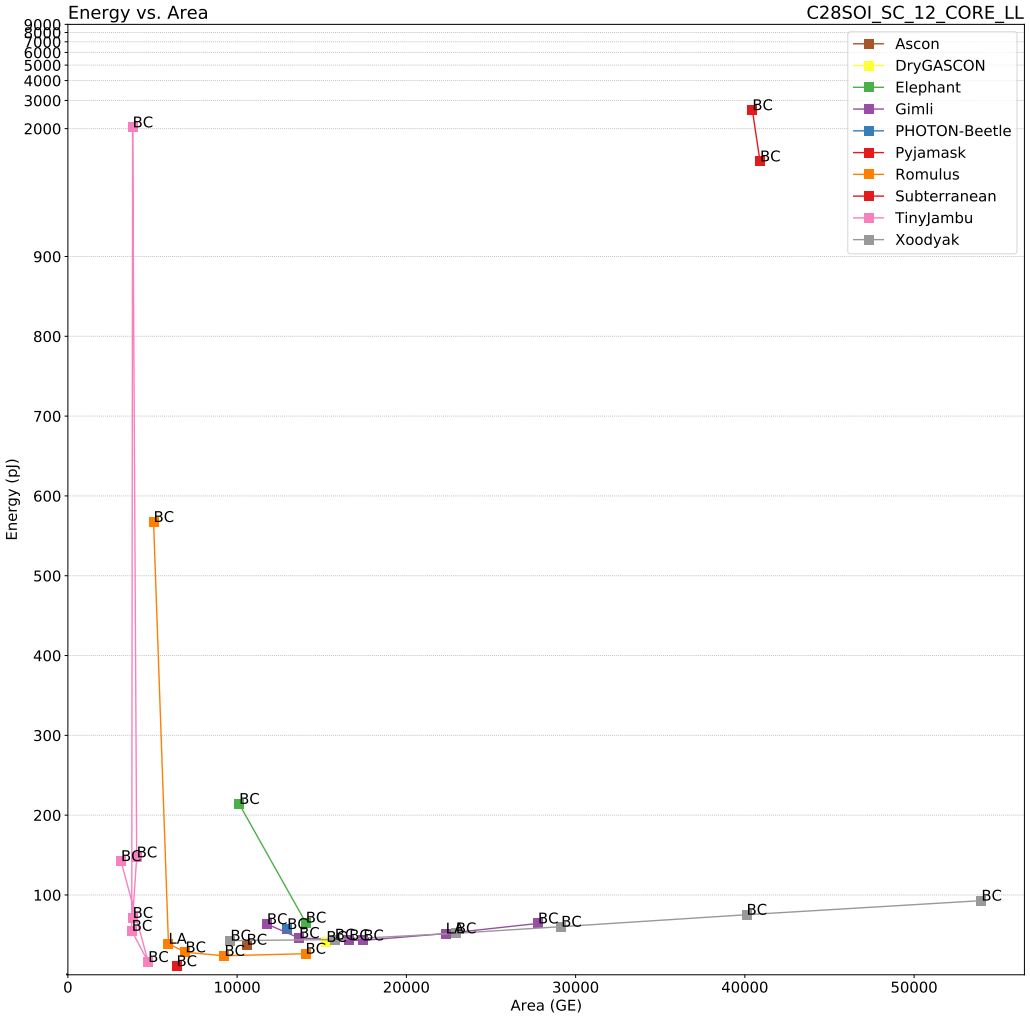

Figure 102: Energy vs. Area for $|A| = |M| = 16$ bytes on FDSOI 28nm. The energy axis follows a log scale for values $\geqslant 900$ pJ.

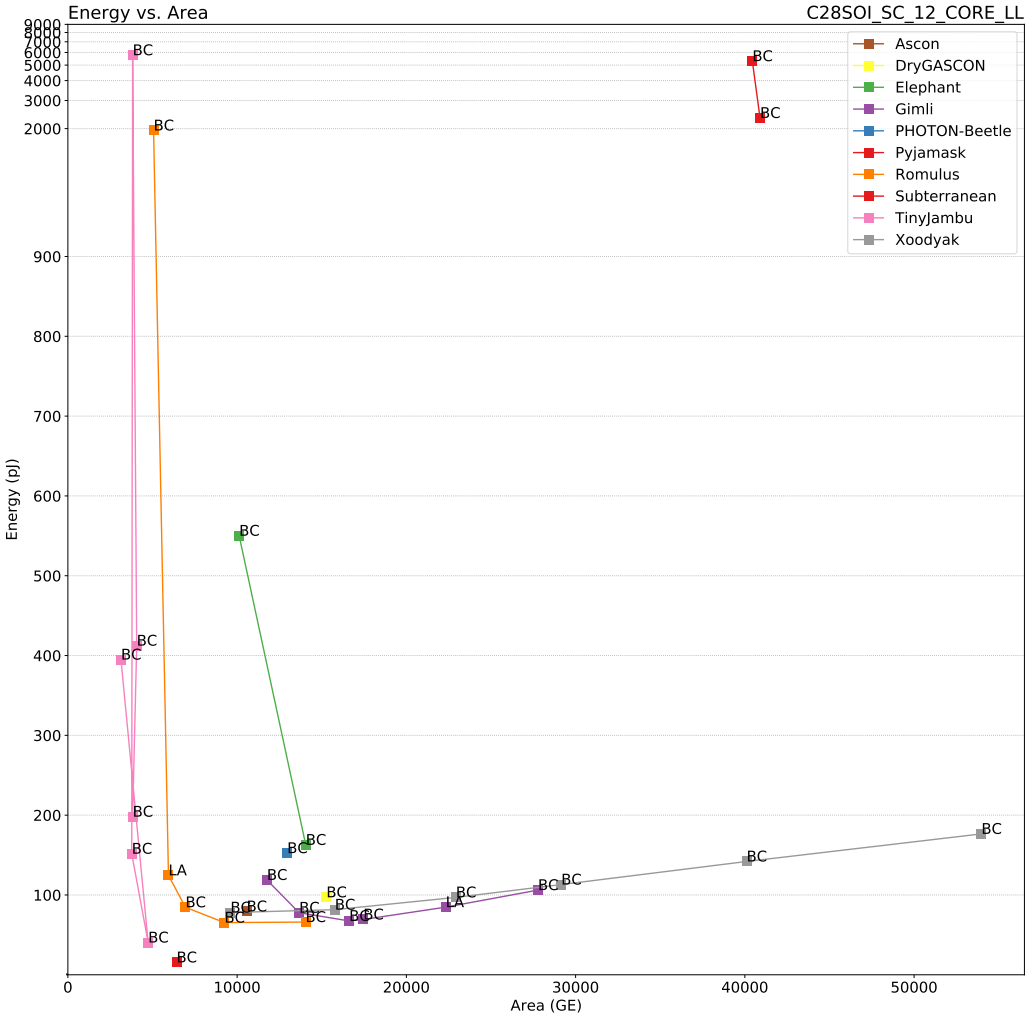

Figure 103: Energy vs. Area for $|A| = |M| = 64$ bytes on FDSOI 28nm. The energy axis follows a log scale for values $\geqslant 900$ pJ.

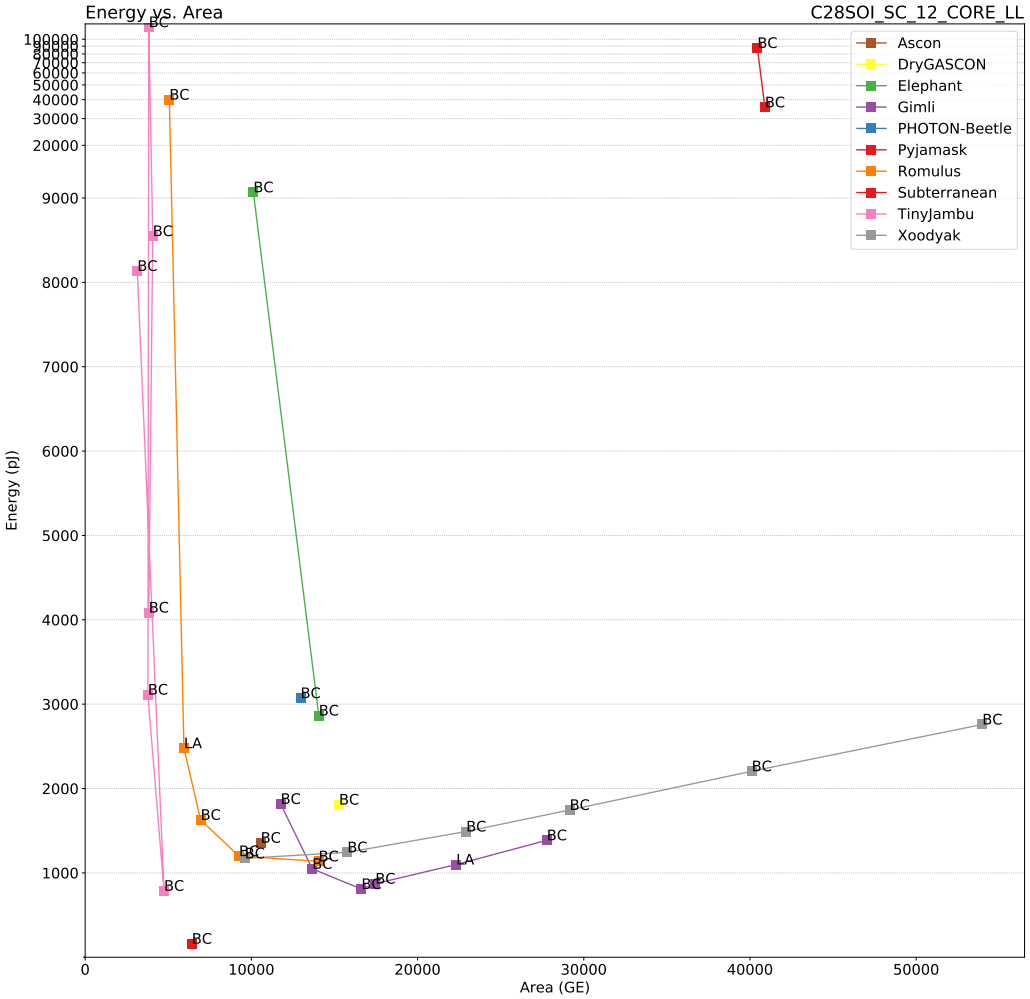

Figure 104: Energy vs. Area for |A| = |M| = 1536 bytes on FDSOI 28nm. The energy axis follows a log scale for values ⩾ 9000 pJ.

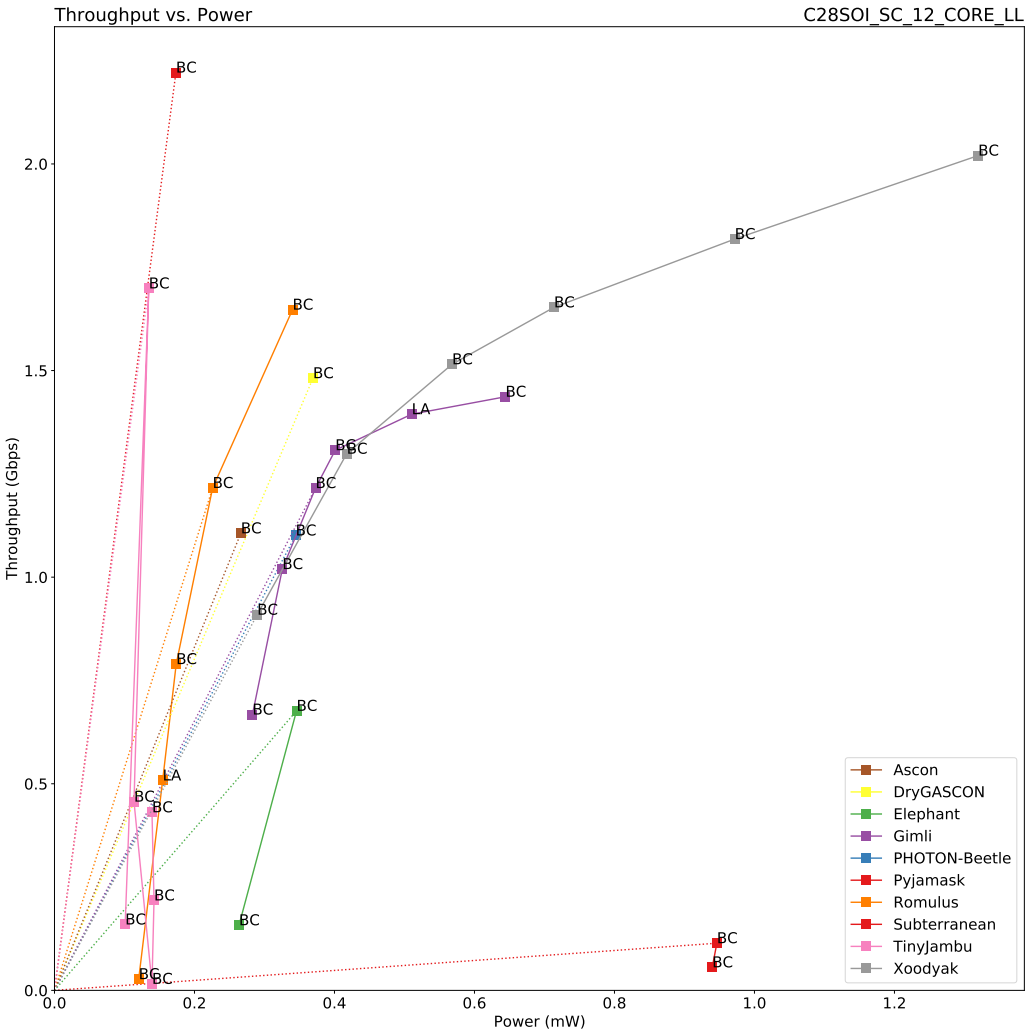

Figure 105: Throughput vs. Power for $|A| = 16$ bytes on FDSOI 28nm.

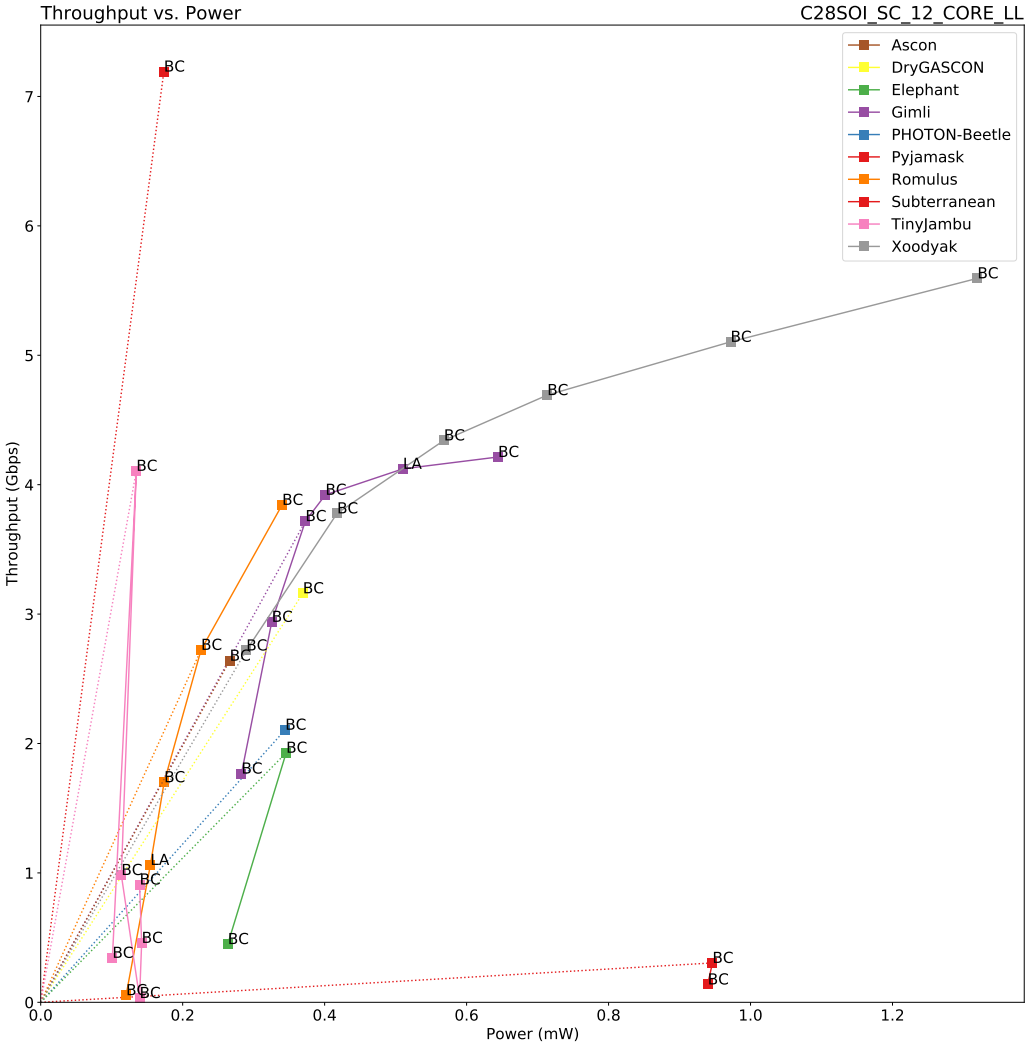

Figure 106: Throughput vs. Power for |A| = 64 bytes on FDSOI 28nm.

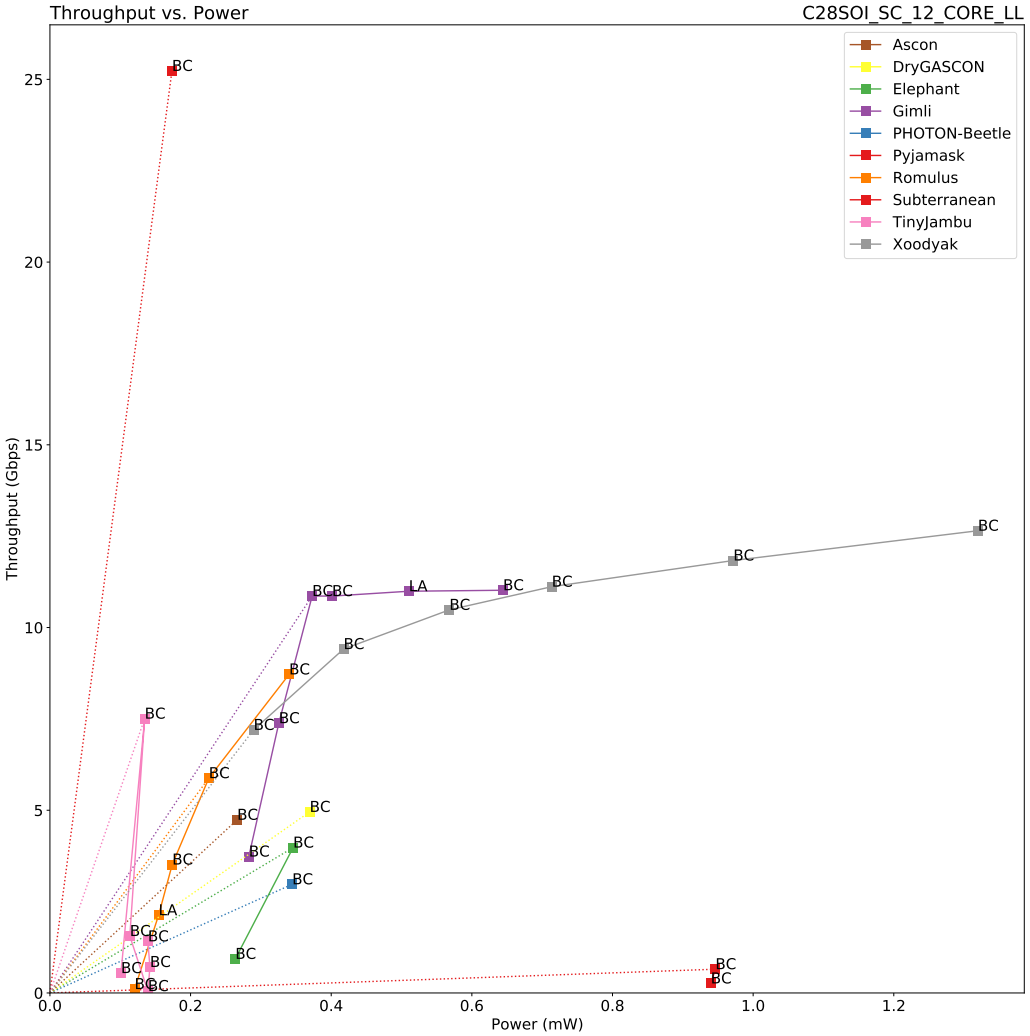

Figure 107: Throughput vs. Power for $|A| = 1536$ bytes on FDSOI 28nm.

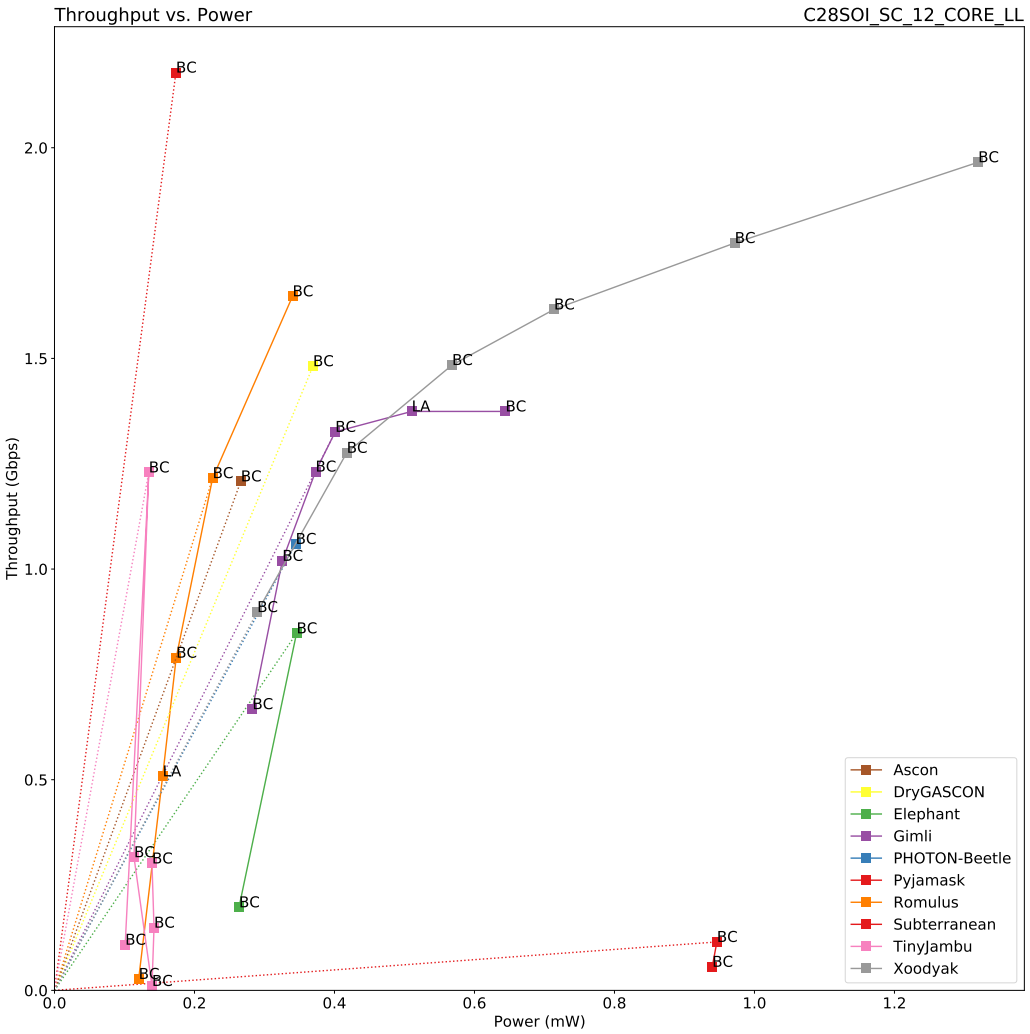

Figure 108: Throughput vs. Power for |M| = 16 bytes on FDSOI 28nm.

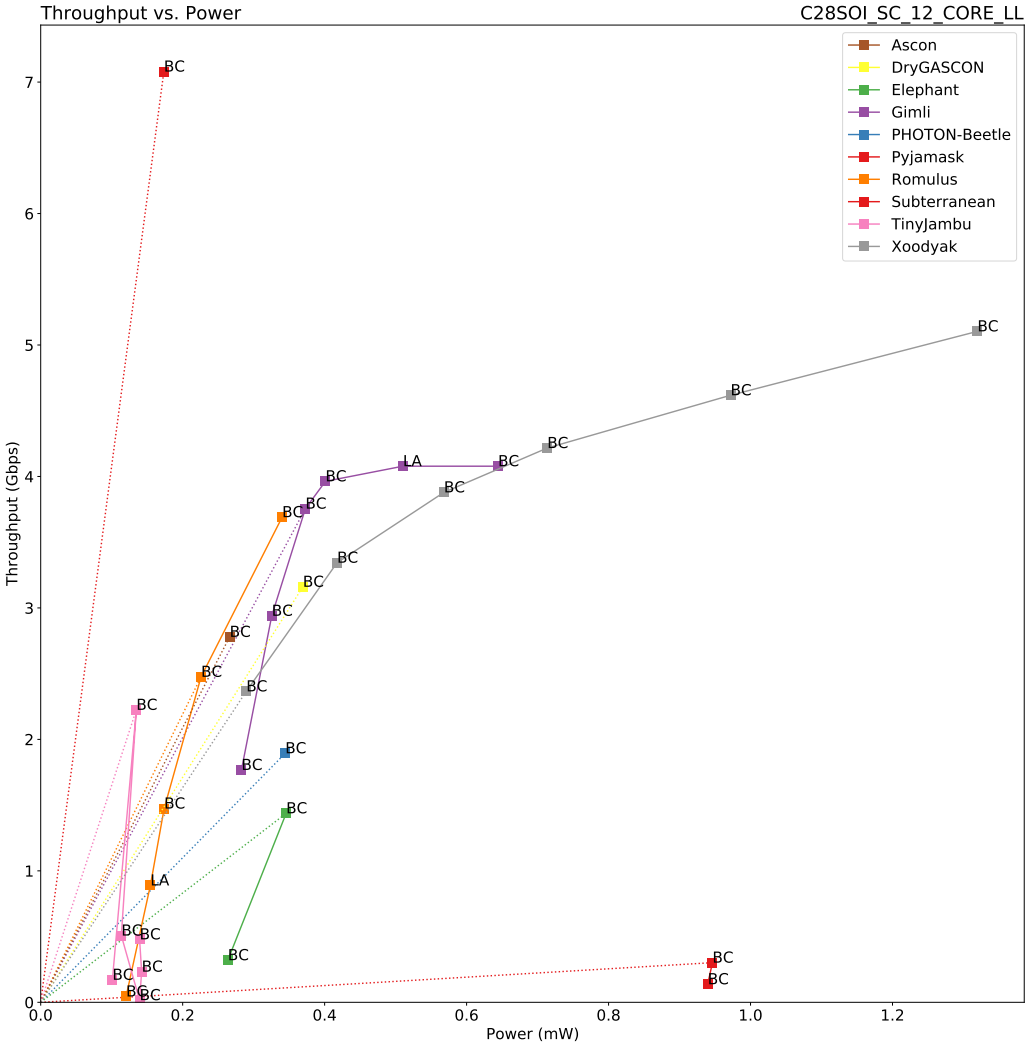

Figure 109: Throughput vs. Power for |M| = 64 bytes on FDSOI 28nm.

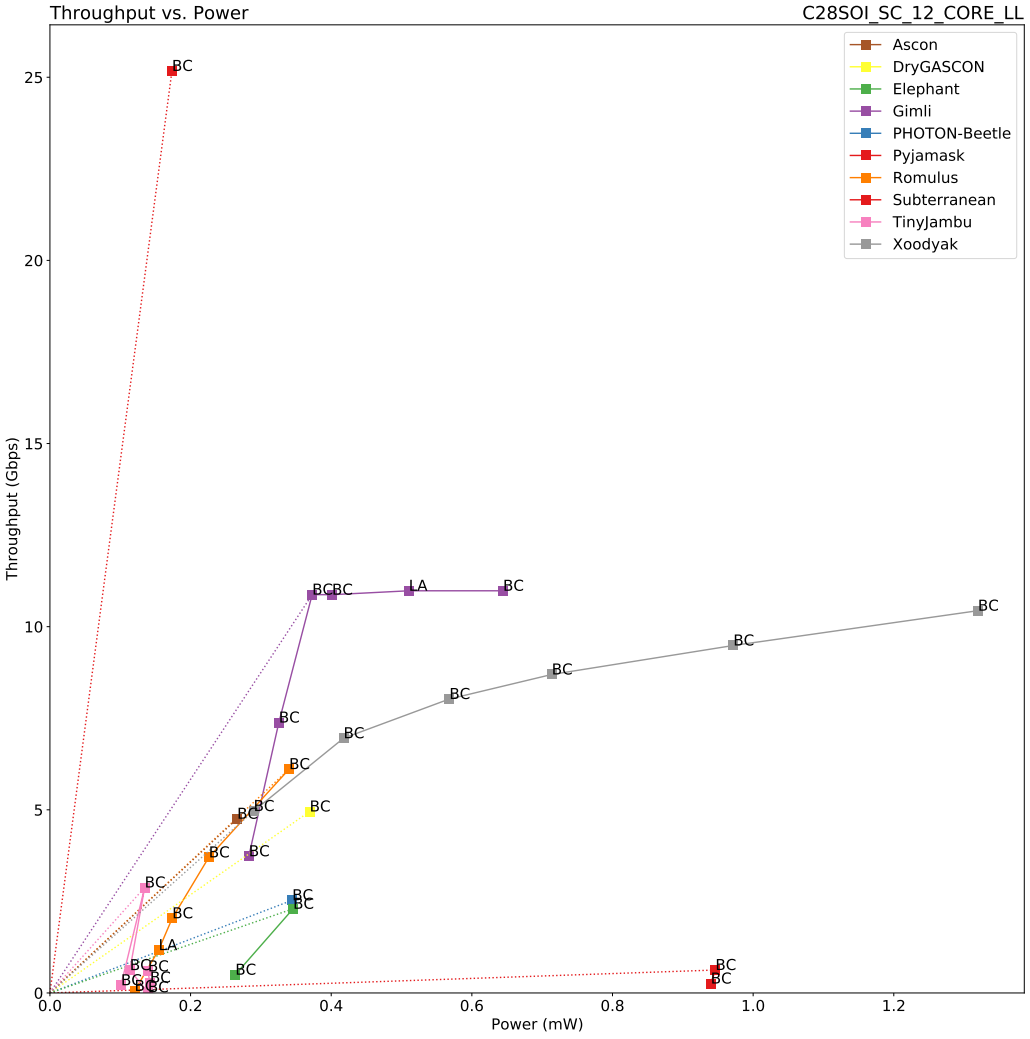

Figure 110: Throughput vs. Power for $|M| = 1536$ bytes on FDSOI 28nm.

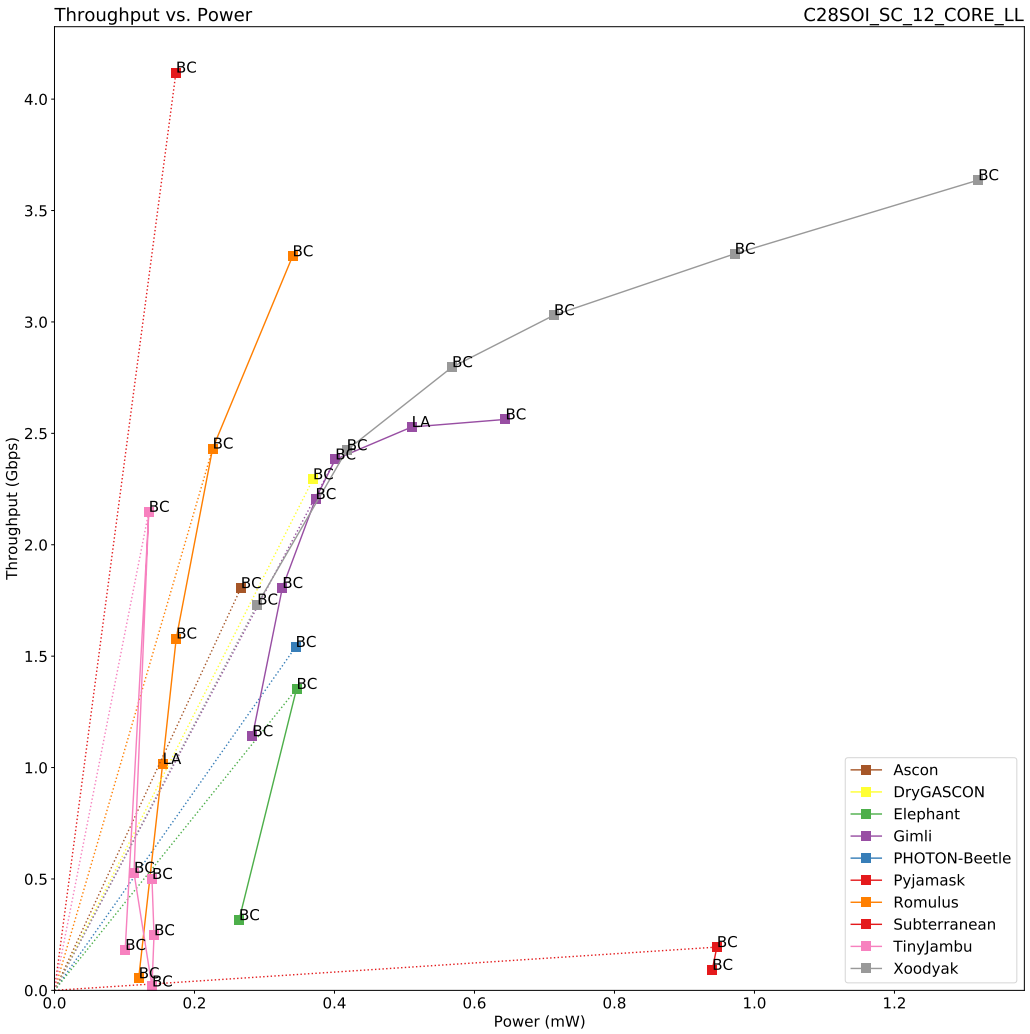

Figure 111: Throughput vs. Power for $|A| = |M| = 16$ bytes on FDSOI 28nm.

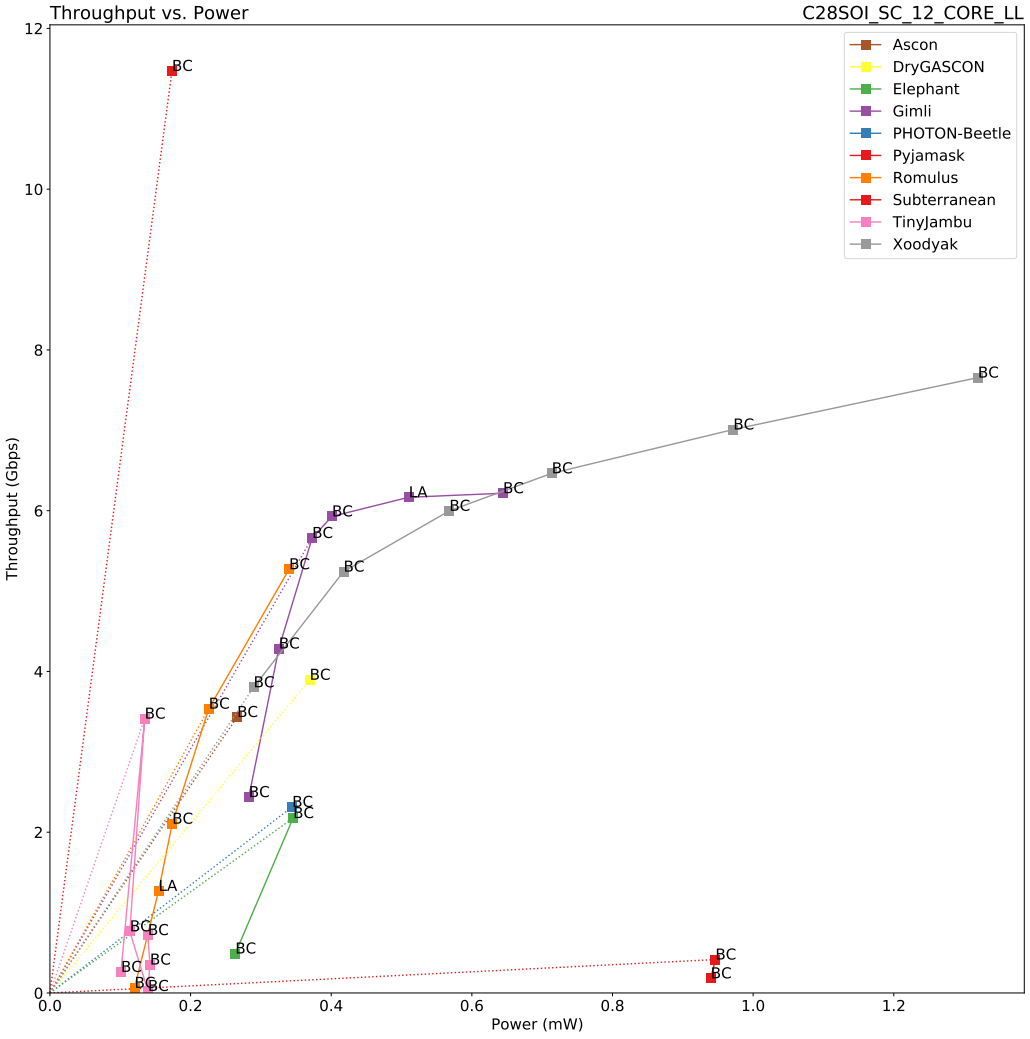

Figure 112: Throughput vs. Power for |A| = |M| = 64 bytes on FDSOI 28nm.

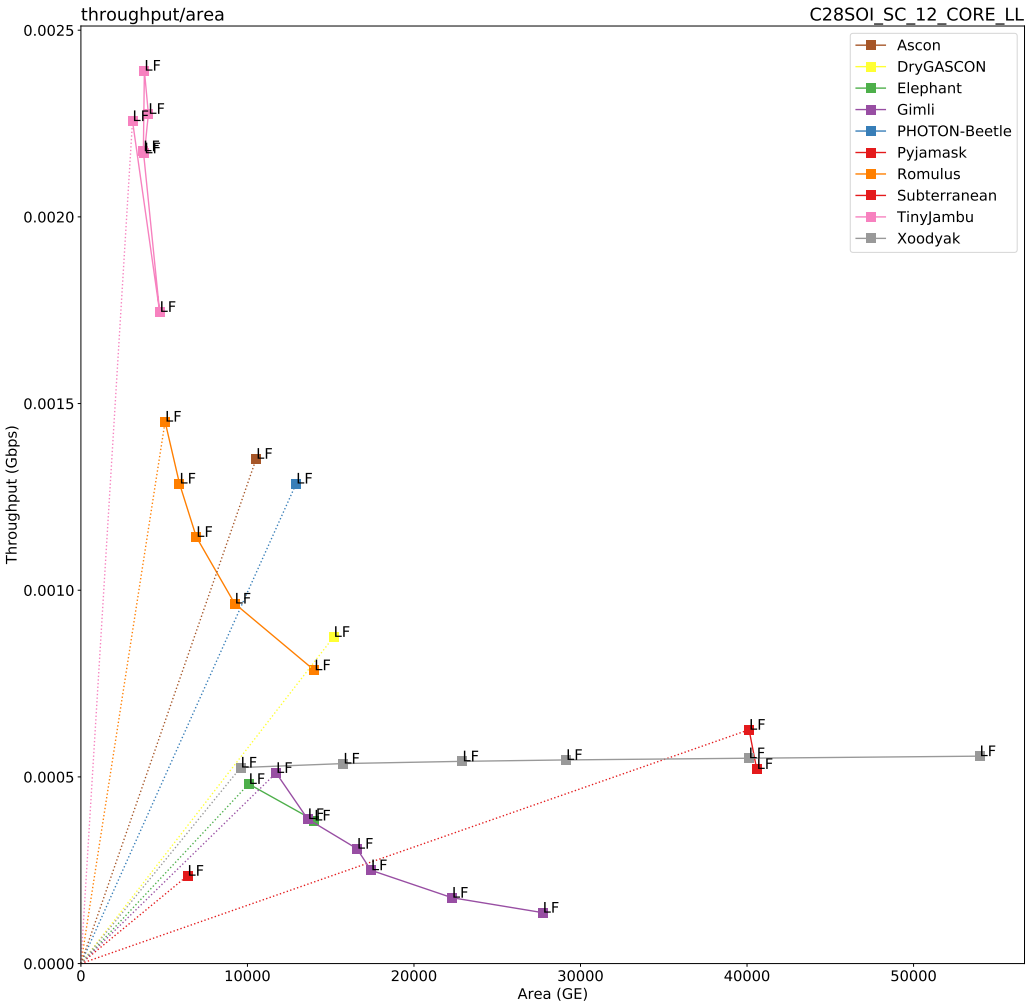

Figure 113: 3 Mbps: Throughput vs. Area for $|A| = 16$ bytes on FDSOI 28nm.

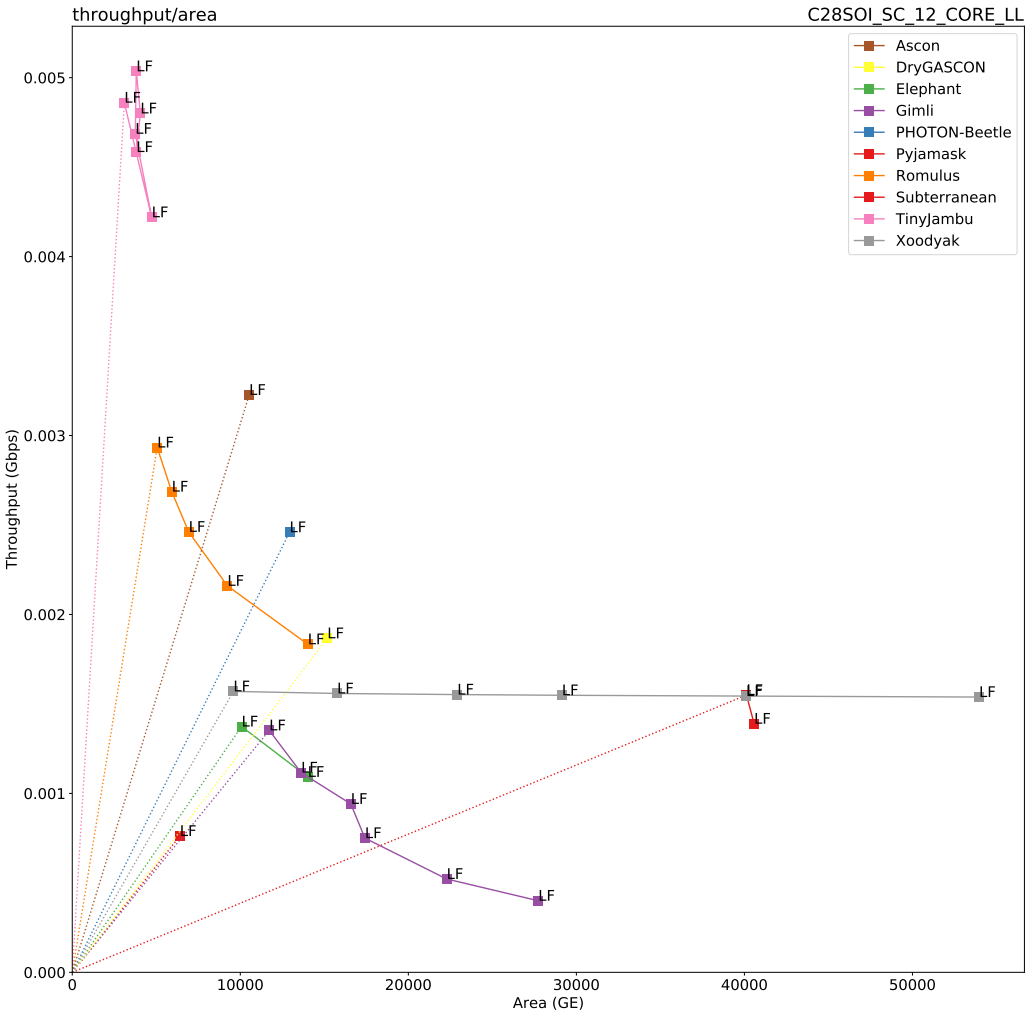

Figure 114: 3 Mbps: Throughput vs. Area for |A| = 64 bytes on FDSOI 28nm.

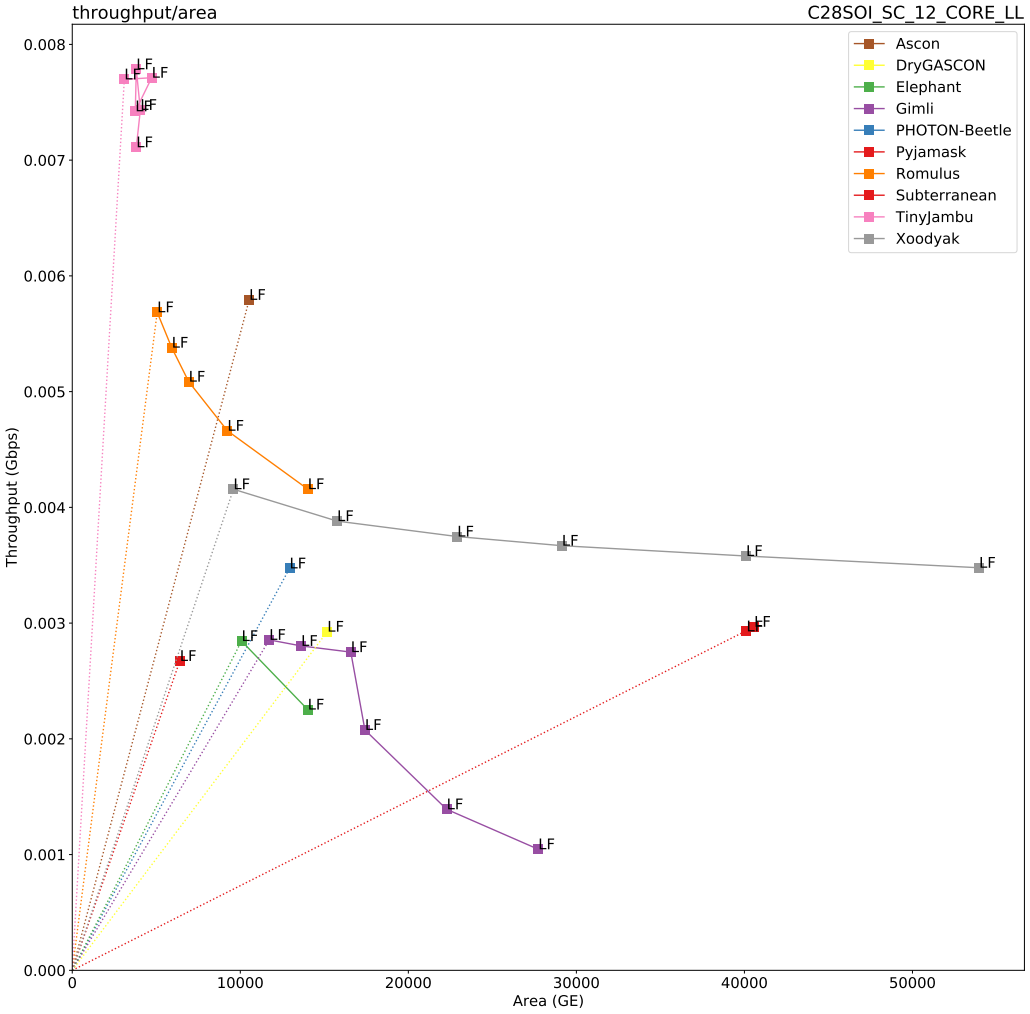

Figure 115: 3 Mbps: Throughput vs. Area for |A| = 1536 bytes on FDSOI 28nm.

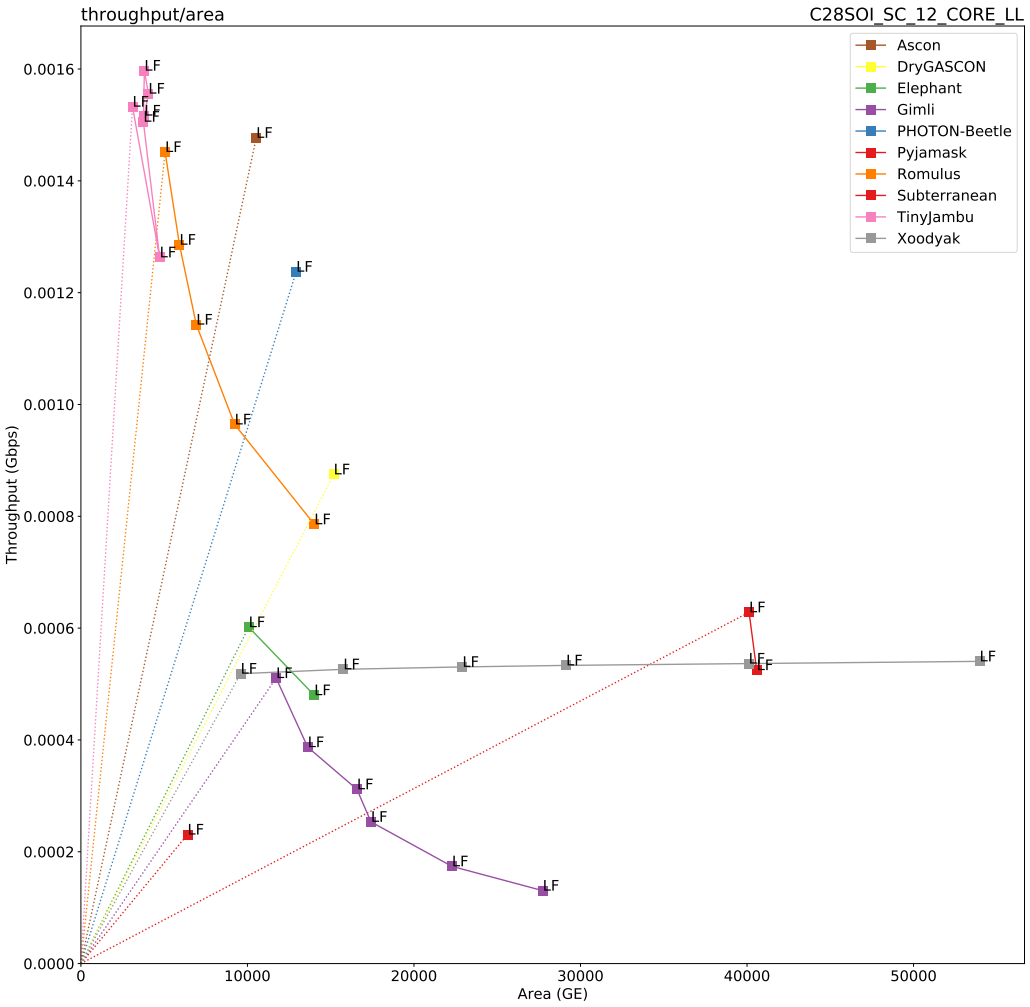

Figure 116: 3 Mbps: Throughput vs. Area for |M| = 16 bytes on FDSOI 28nm.

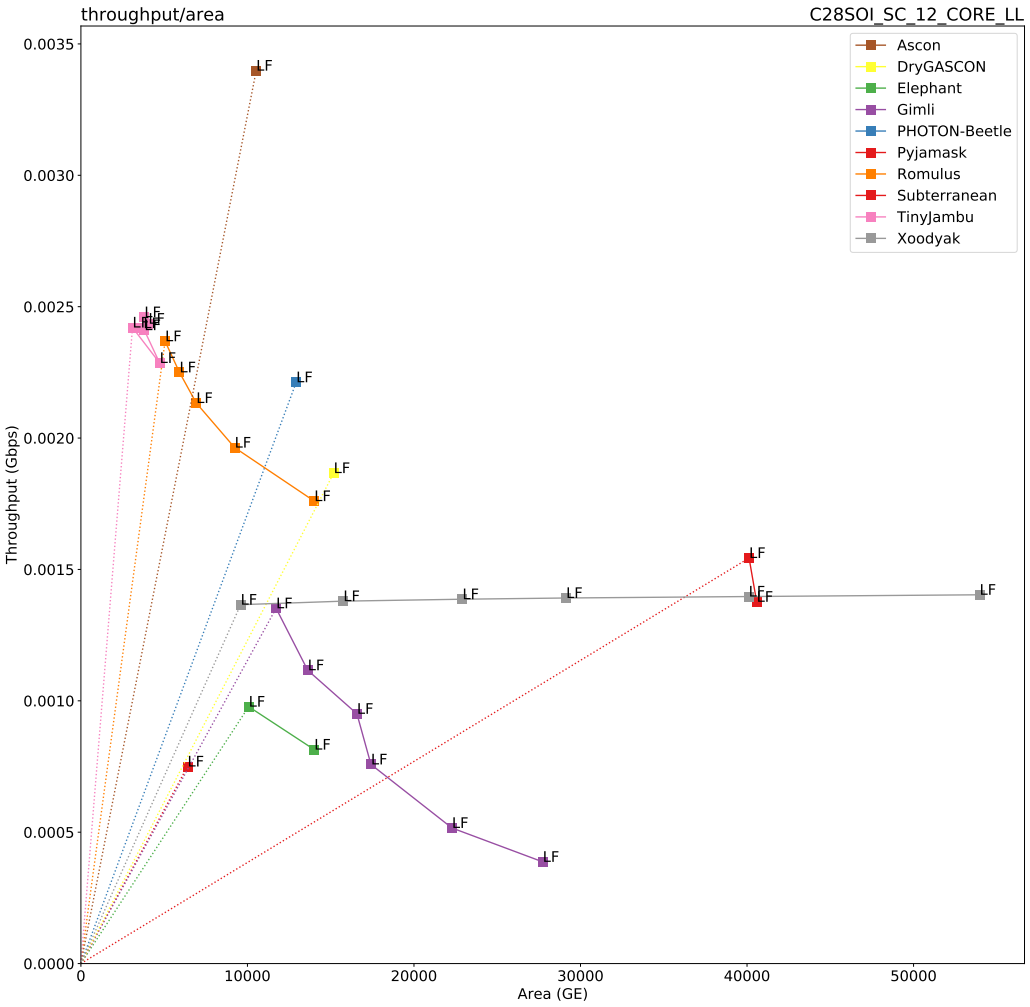

Figure 117: 3 Mbps: Throughput vs. Area for |M| = 64 bytes on FDSOI 28nm.

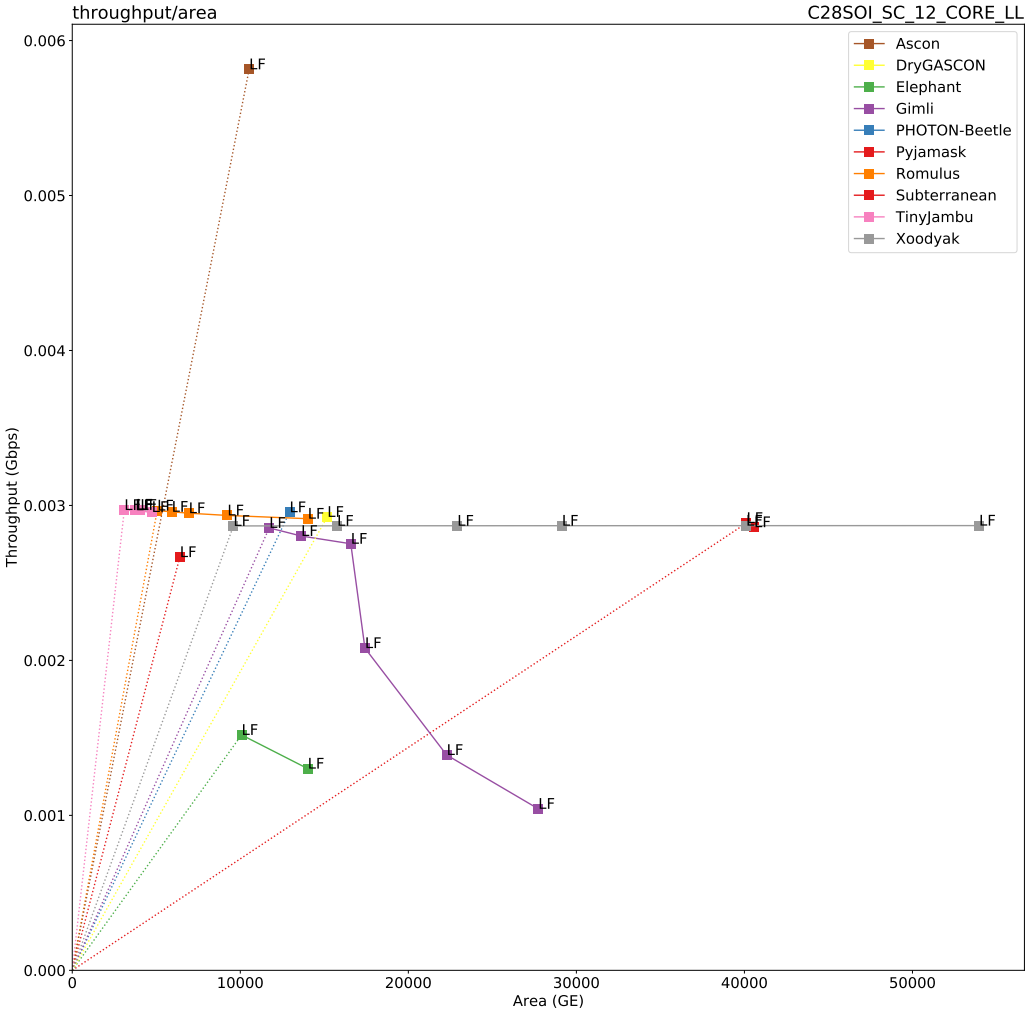

Figure 118: 3 Mbps: Throughput vs. Area for |M| = 1536 bytes on FDSOI 28nm.

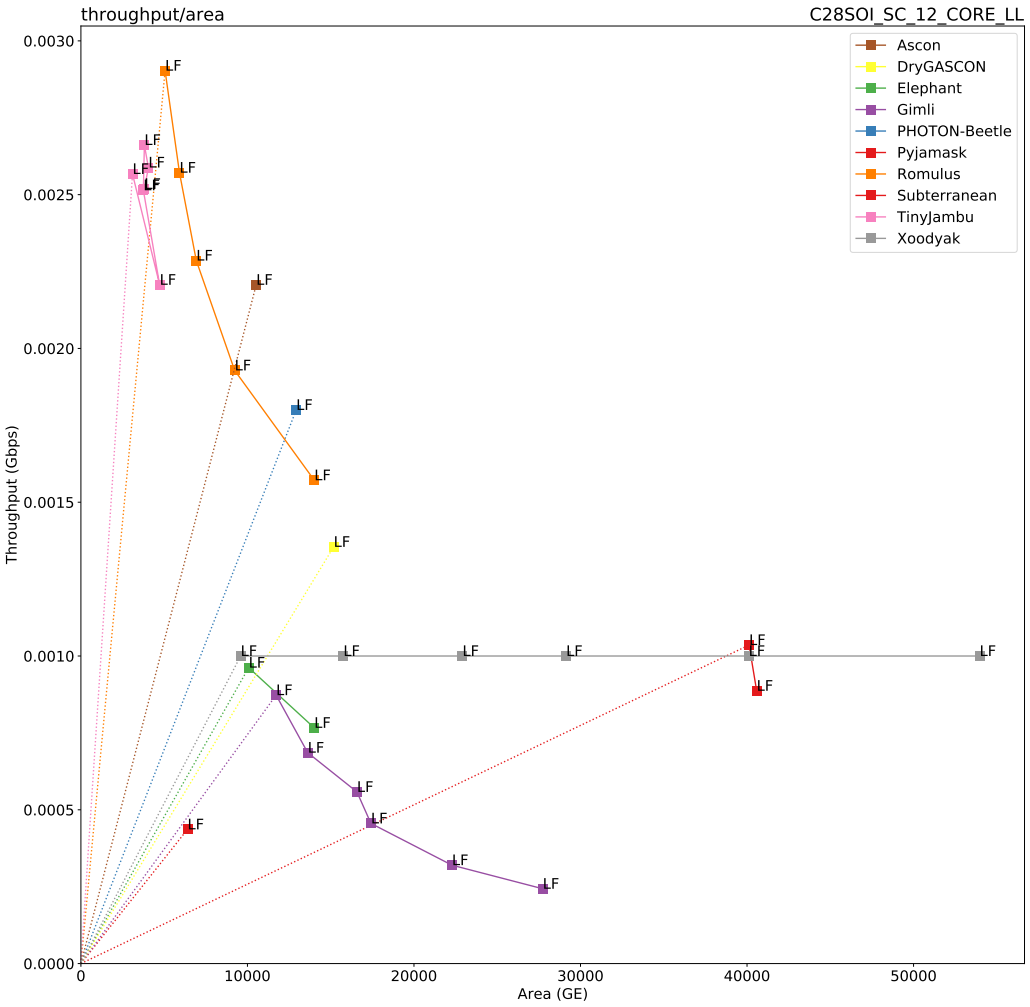

Figure 119: 3 Mbps: Throughput vs. Area for |A| = |M| = 16 bytes on FDSOI 28nm.

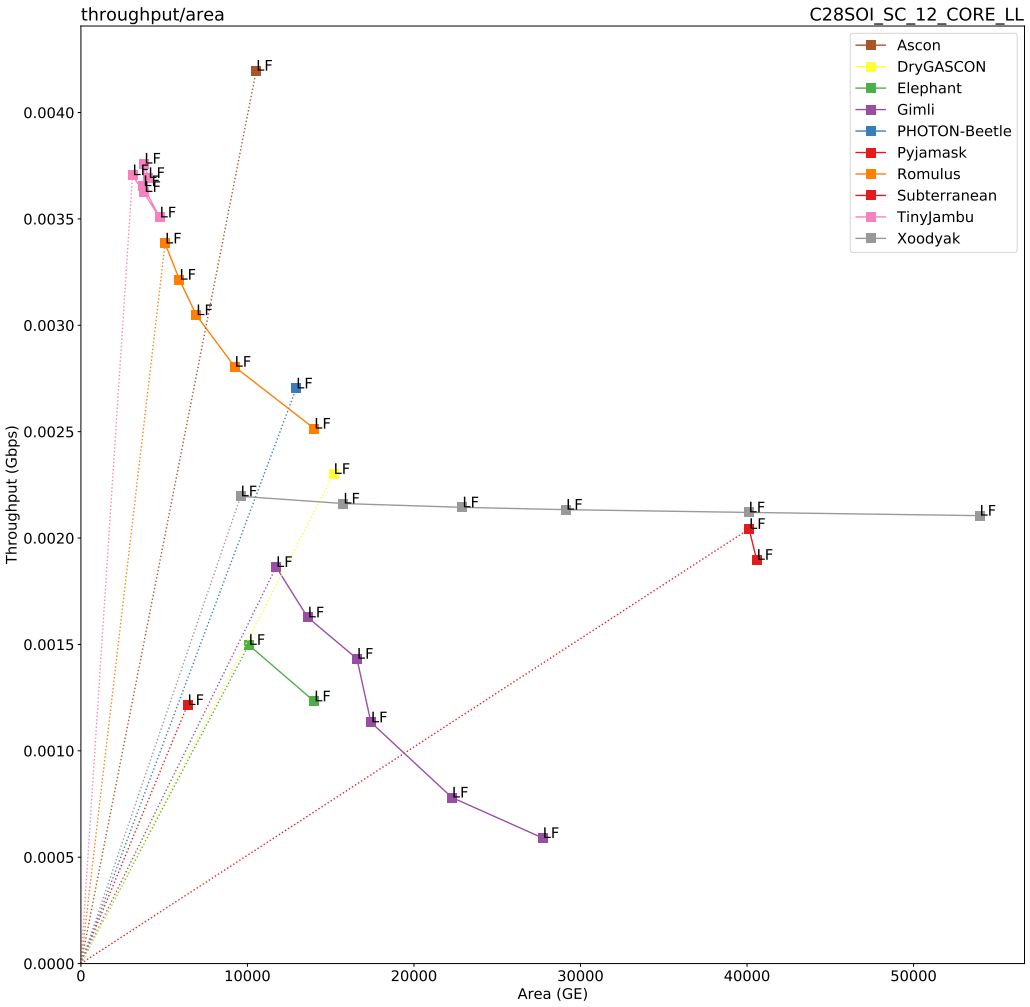

Figure 120: 3 Mbps: Throughput vs. Area for |A| = |M| = 64 bytes on FDSOI 28nm.

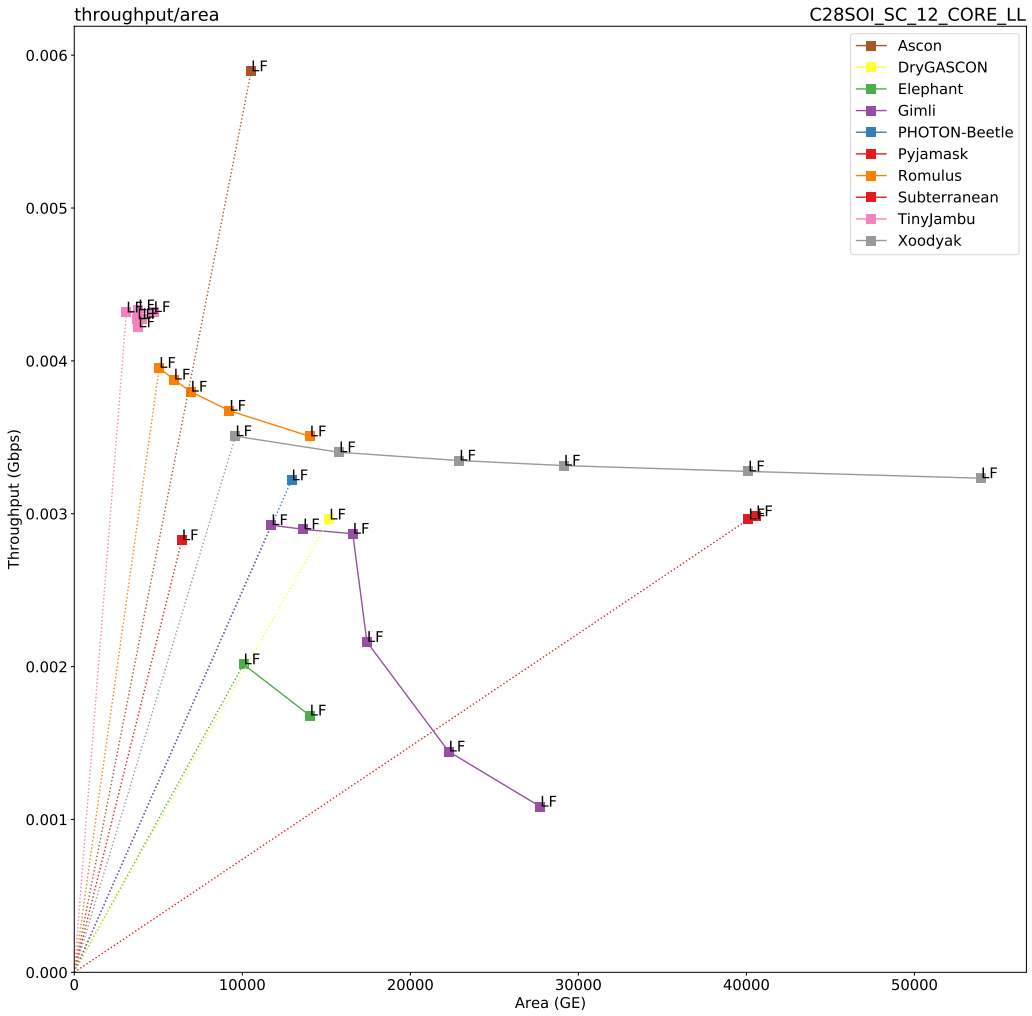

Figure 121: 3 Mbps: Throughput vs. Area for |A| = |M| = 1536 bytes on FDSOI 28nm.

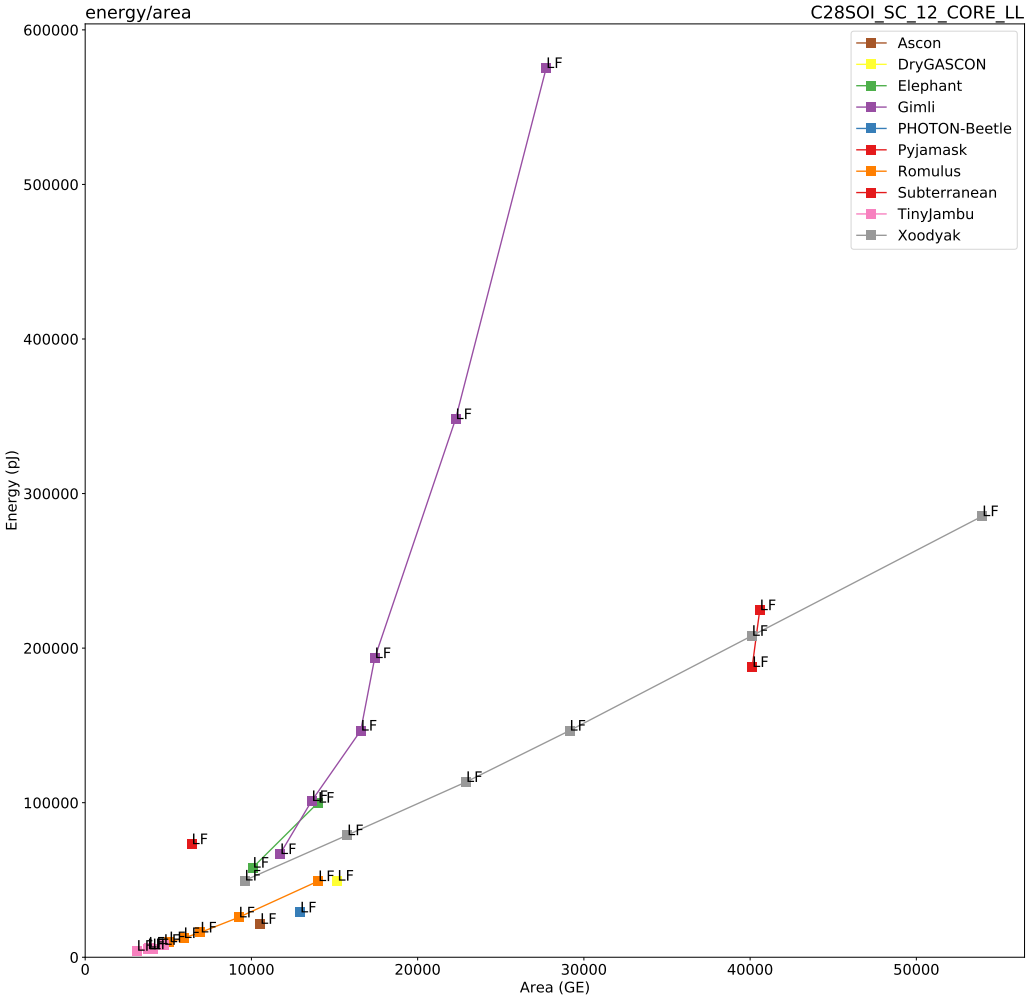

Figure 122: 3 Mbps: Energy vs. Area for |A| = 16 bytes on FDSOI 28nm.

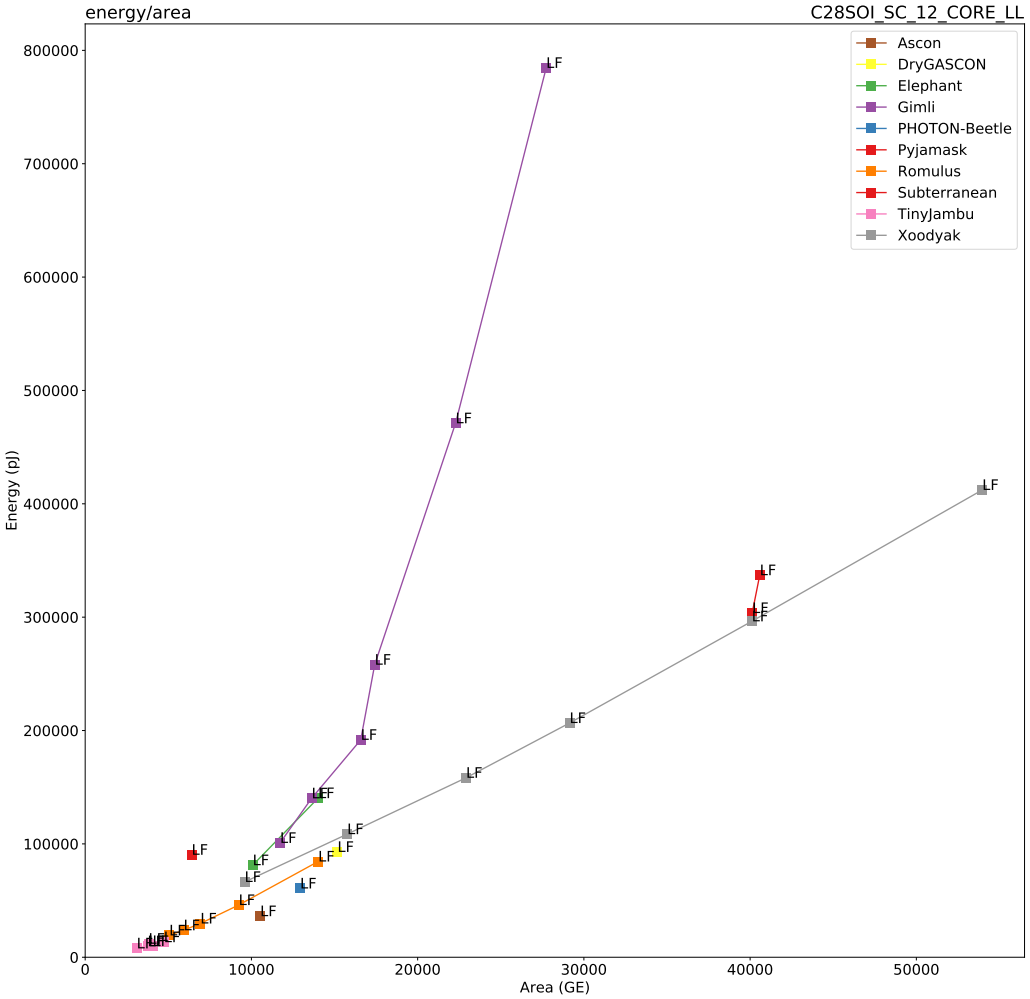

Figure 123: 3 Mbps: Energy vs. Area for $|A| = 64$ bytes on FDSOI 28nm.

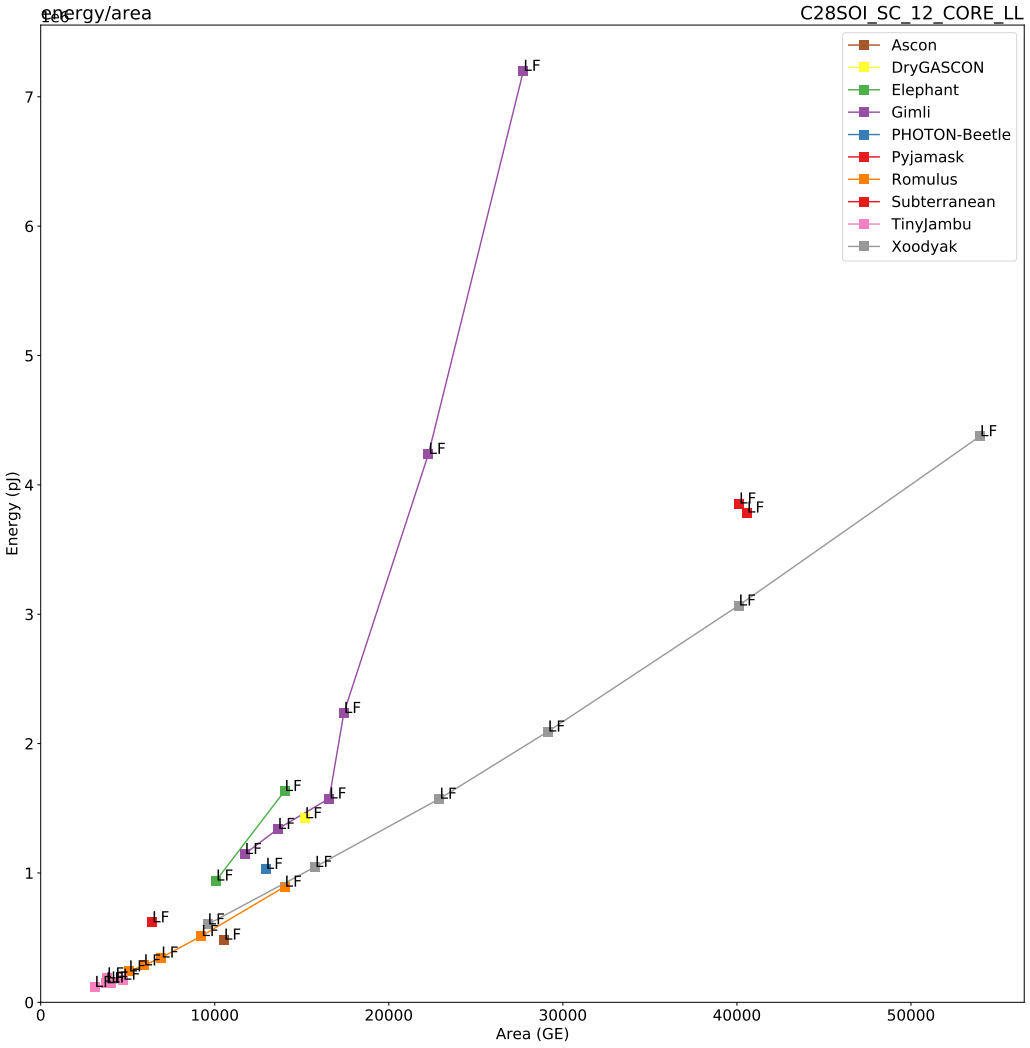

Figure 124: 3 Mbps: Energy vs. Area for |A| = 1536 bytes on FDSOI 28nm.

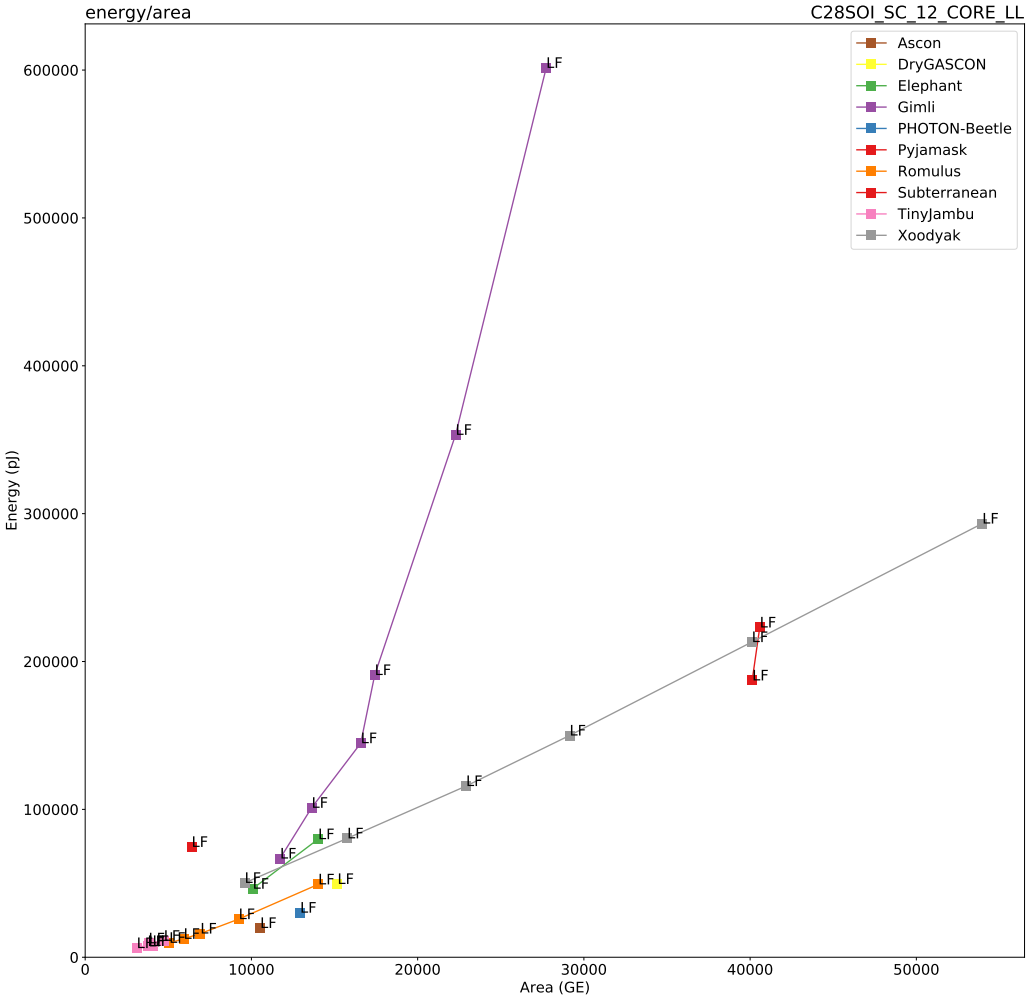

Figure 125: 3 Mbps: Energy vs. Area for |M| = 16 bytes on FDSOI 28nm.

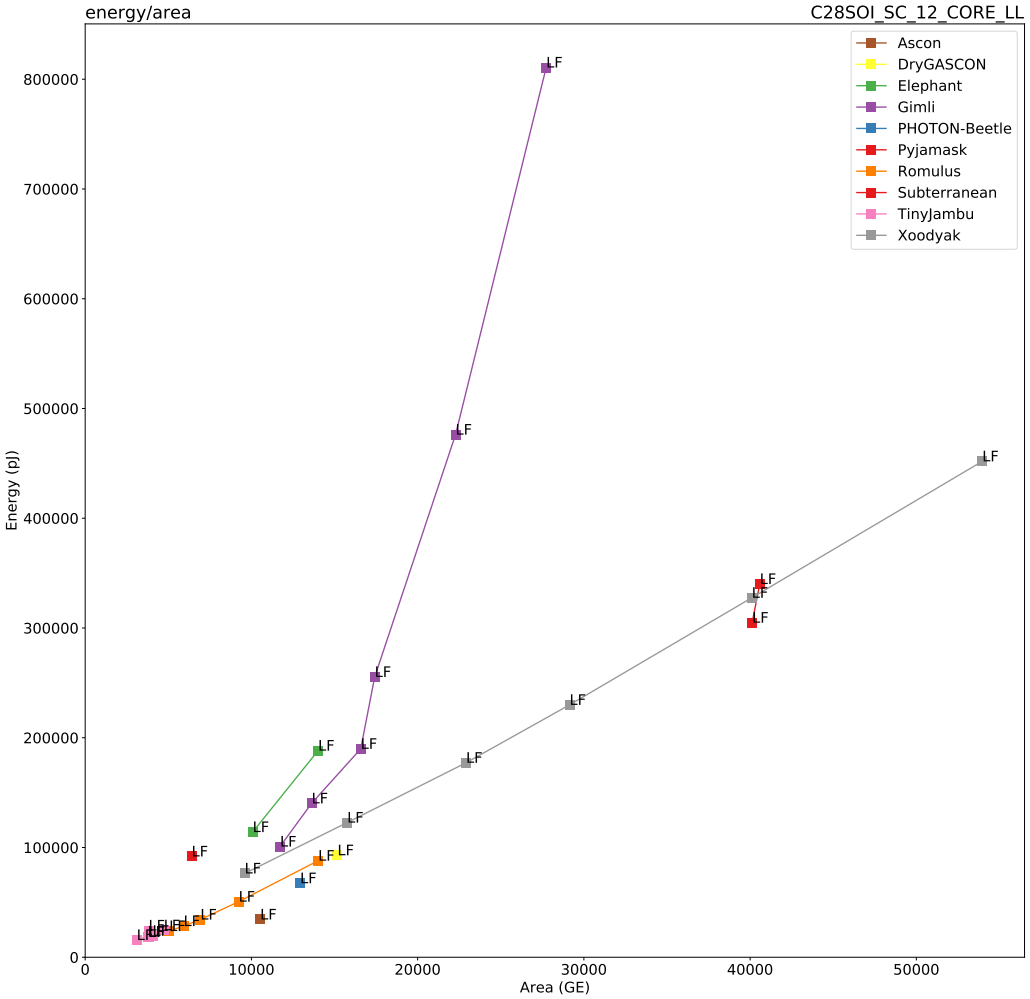

Figure 126: 3 Mbps: Energy vs. Area for |M| = 64 bytes on FDSOI 28nm.

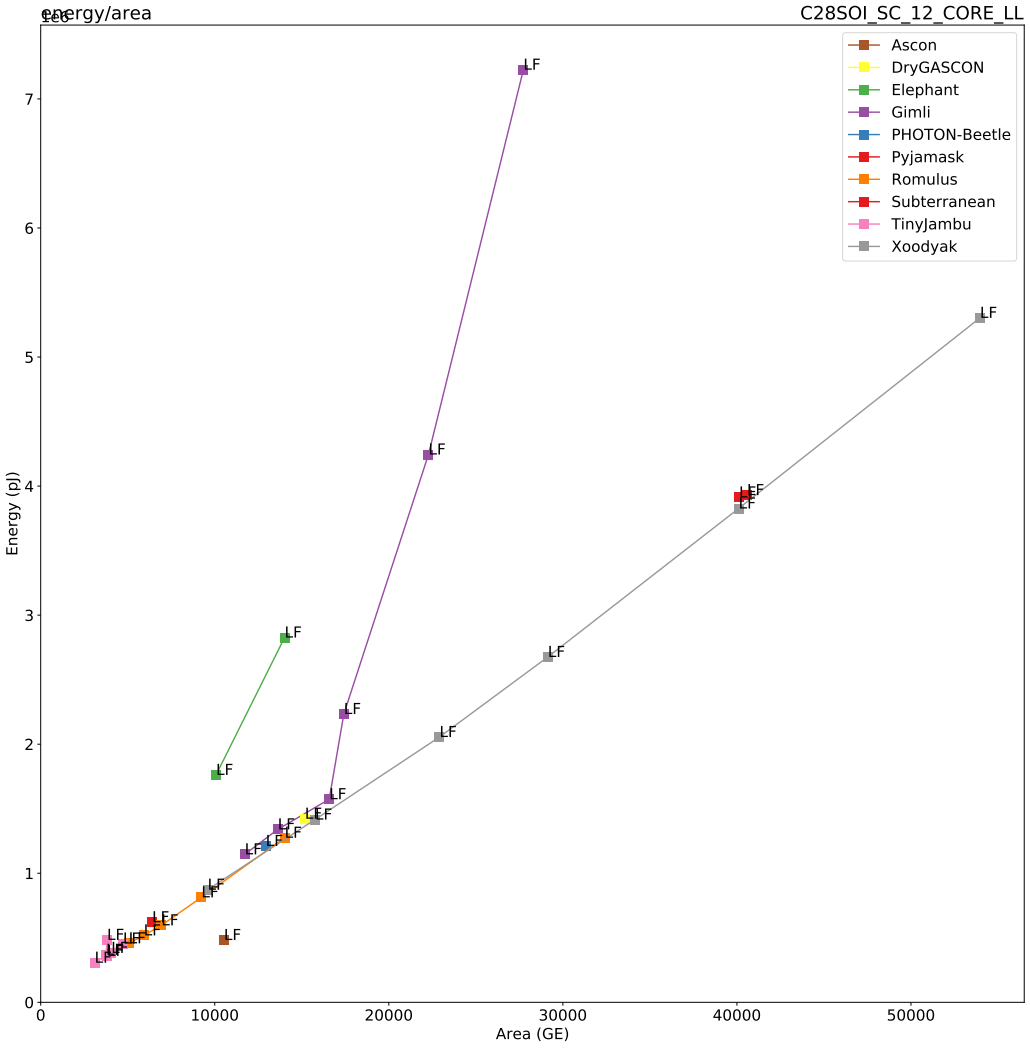

Figure 127: 3 Mbps: Energy vs. Area for $|M| = 1536$ bytes on FDSOI 28nm.

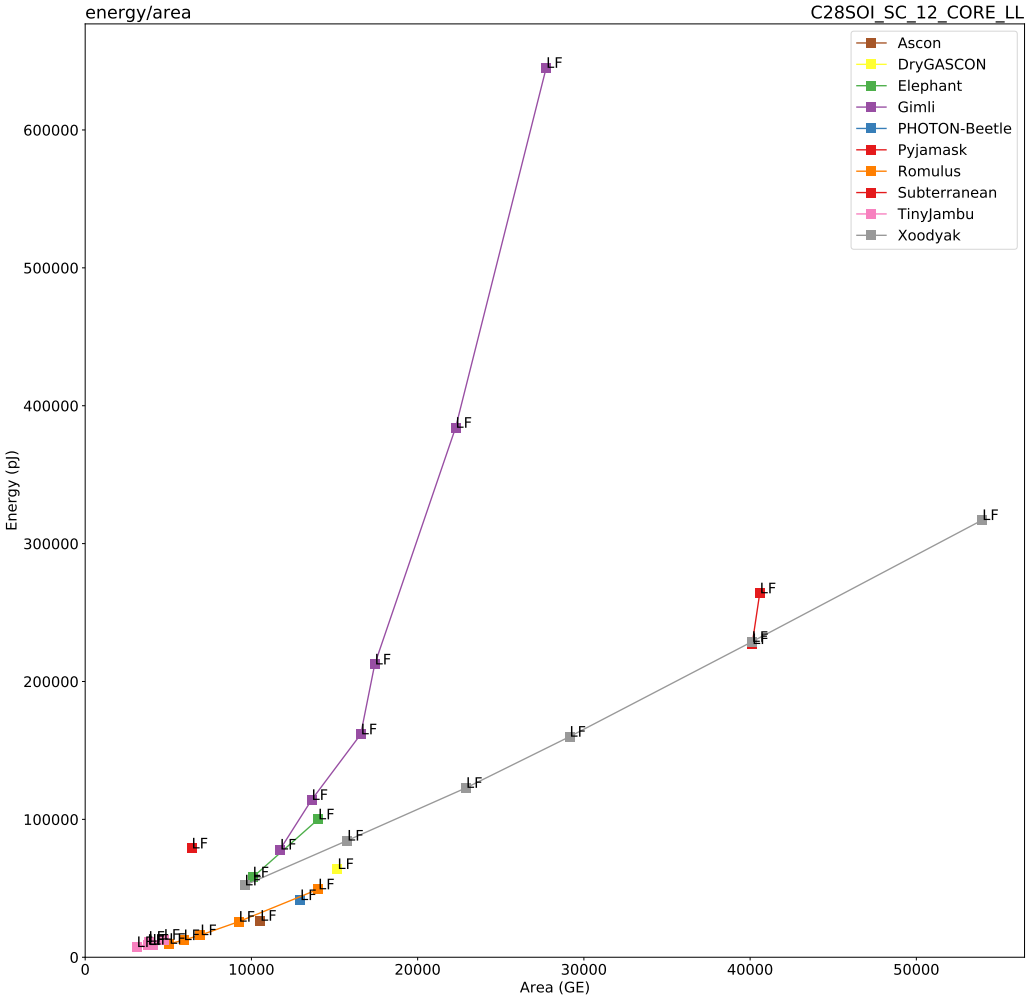

Figure 128: 3 Mbps: Energy vs. Area for |A| = |M| = 16 bytes on FDSOI 28nm.

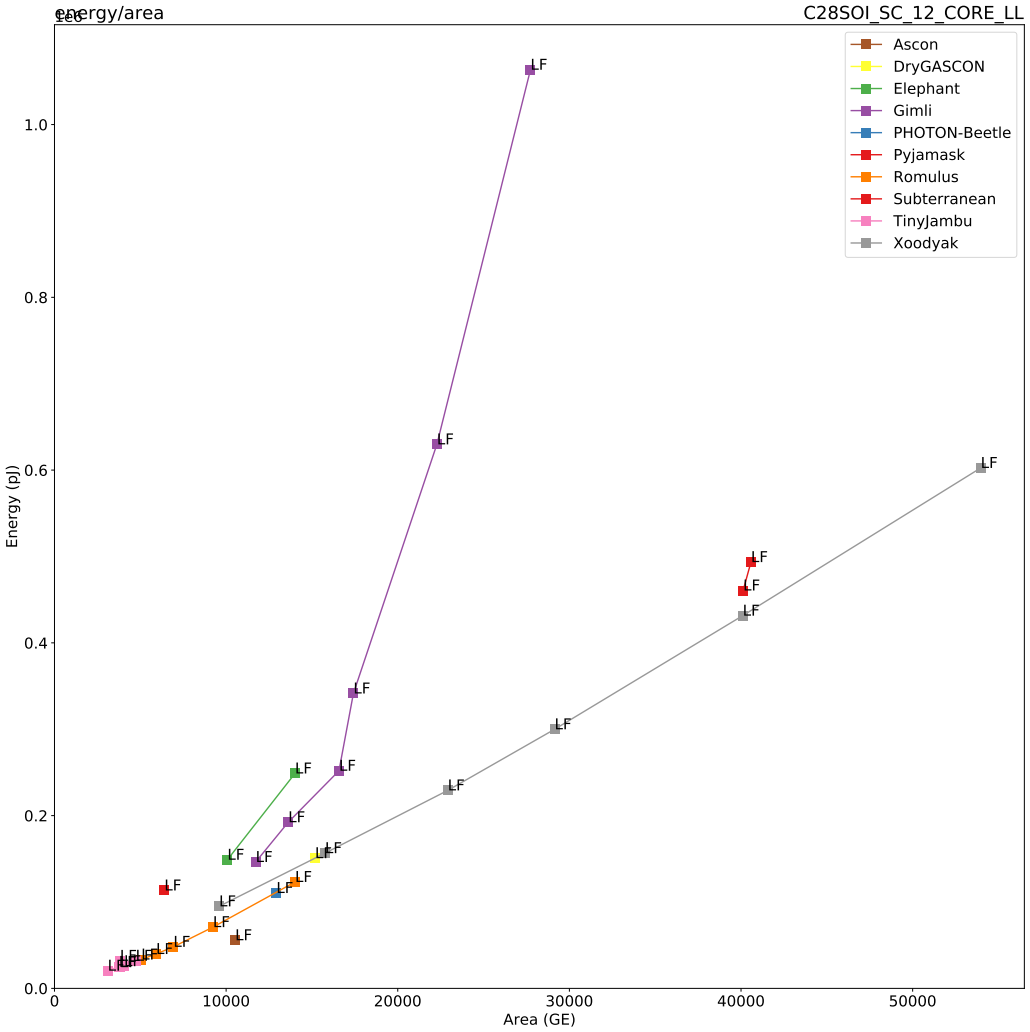

Figure 129: 3 Mbps: Energy vs. Area for |A| = |M| = 64 bytes on FDSOI 28nm.

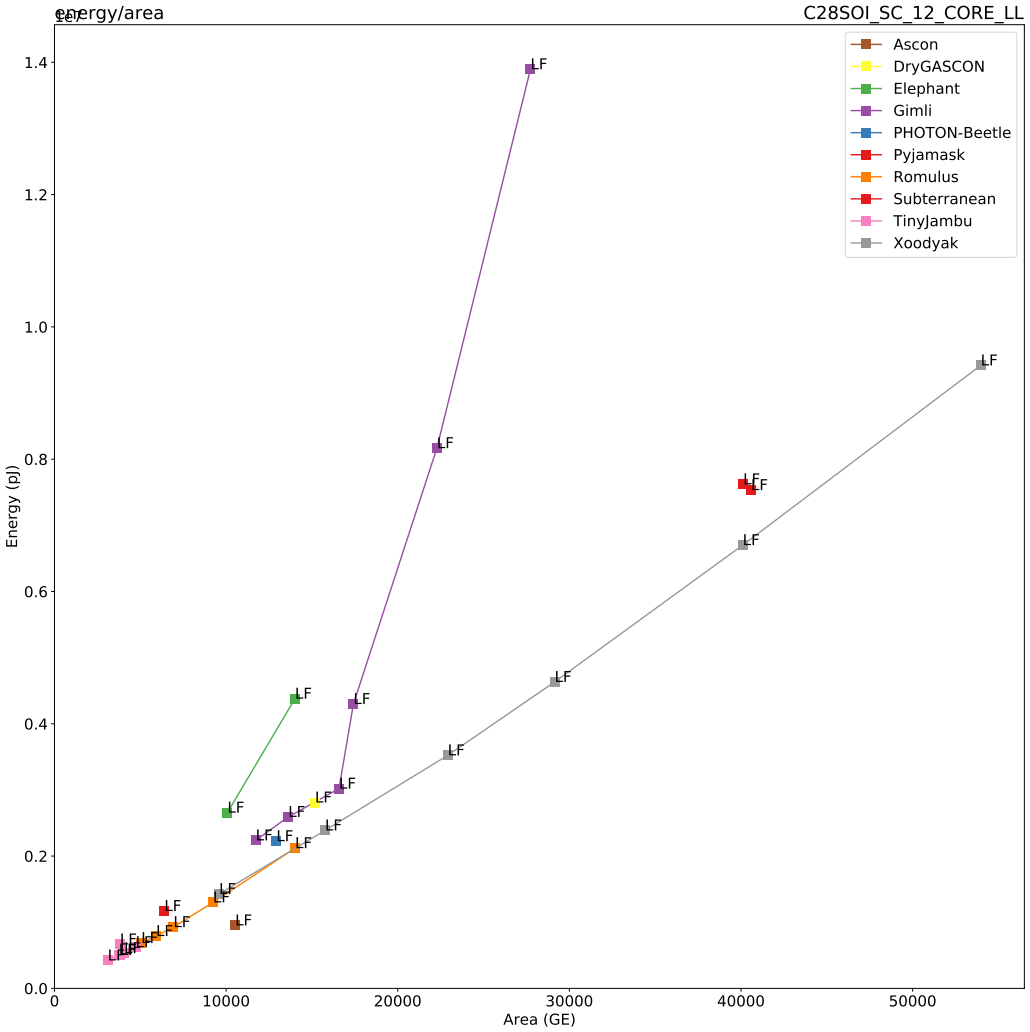

Figure 130: 3 Mbps: Energy vs. Area for |A| = |M| = 1536 bytes on FDSOI 28nm.

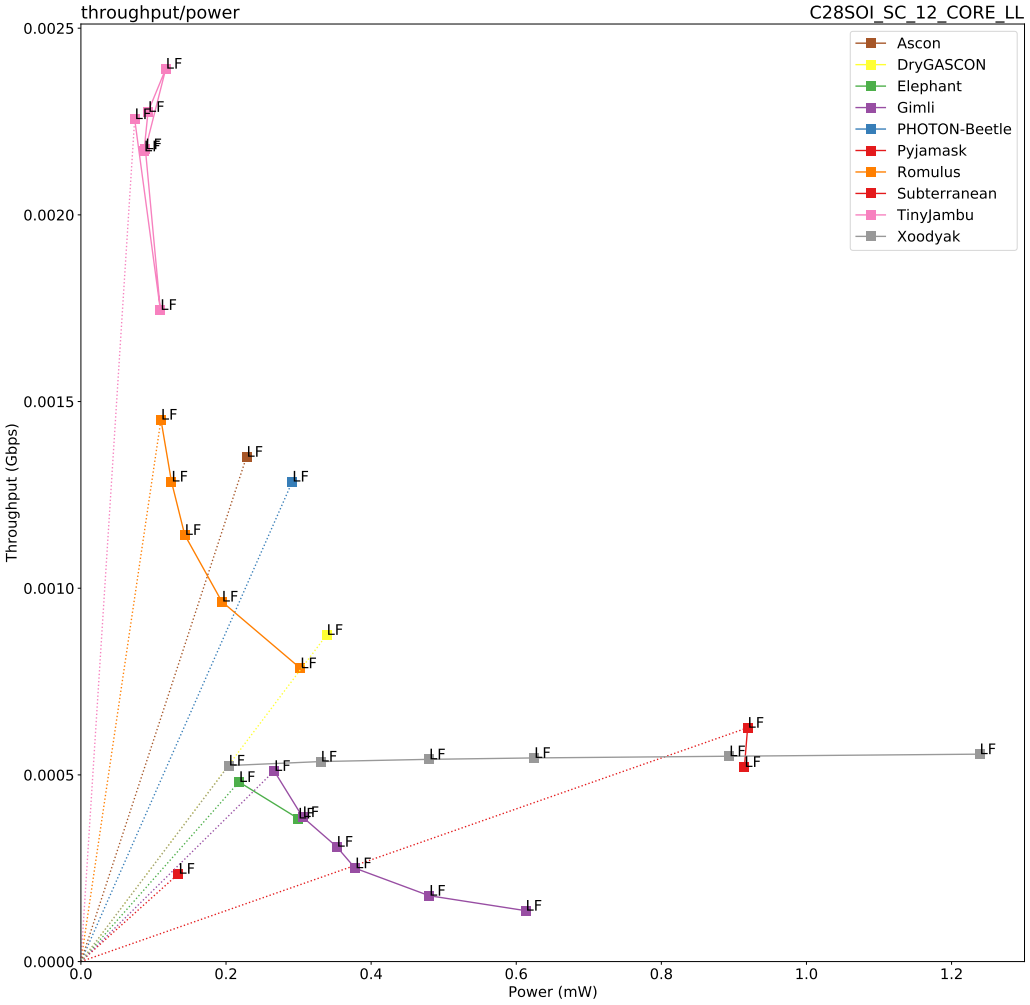

Figure 131: 3 Mbps: Throughput vs. Power for |A| = 16 bytes on FDSOI 28nm.

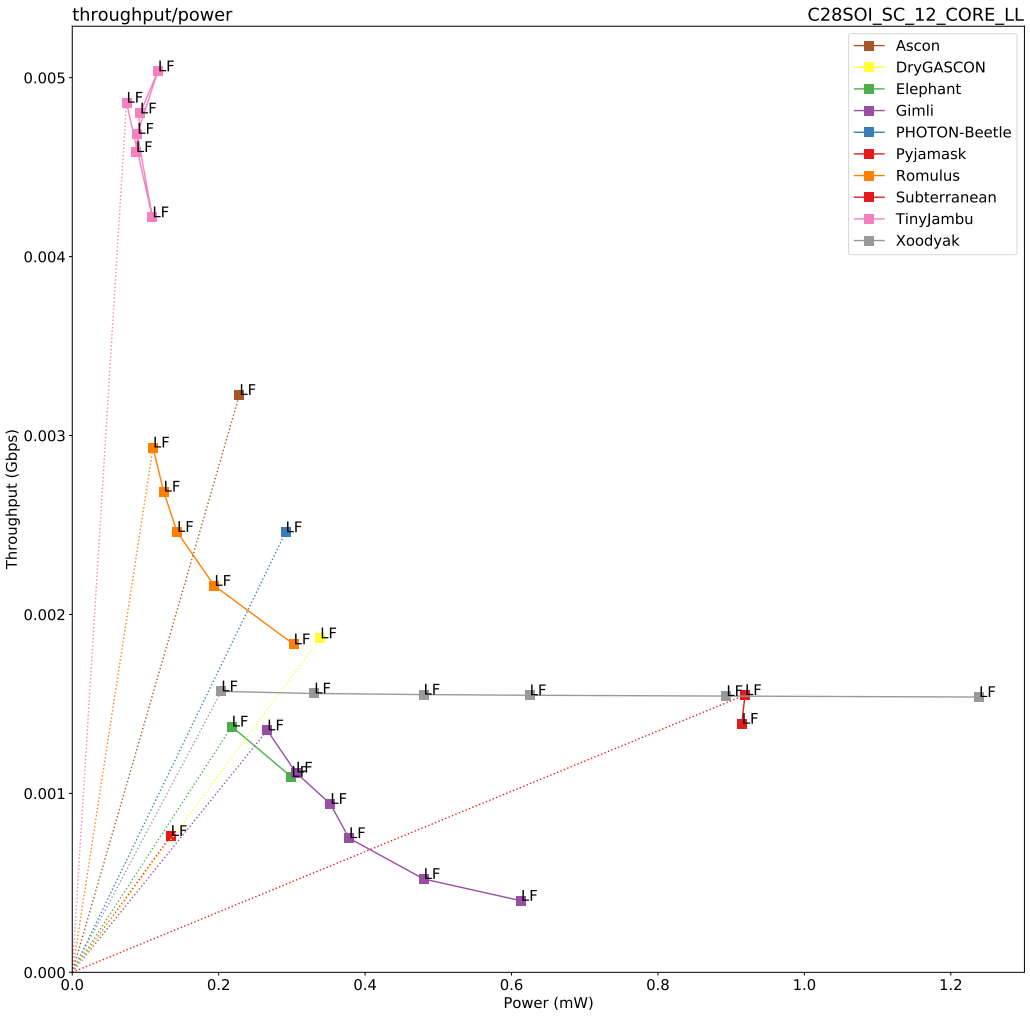

Figure 132: 3 Mbps: Throughput vs. Power for |A| = 64 bytes on FDSOI 28nm.

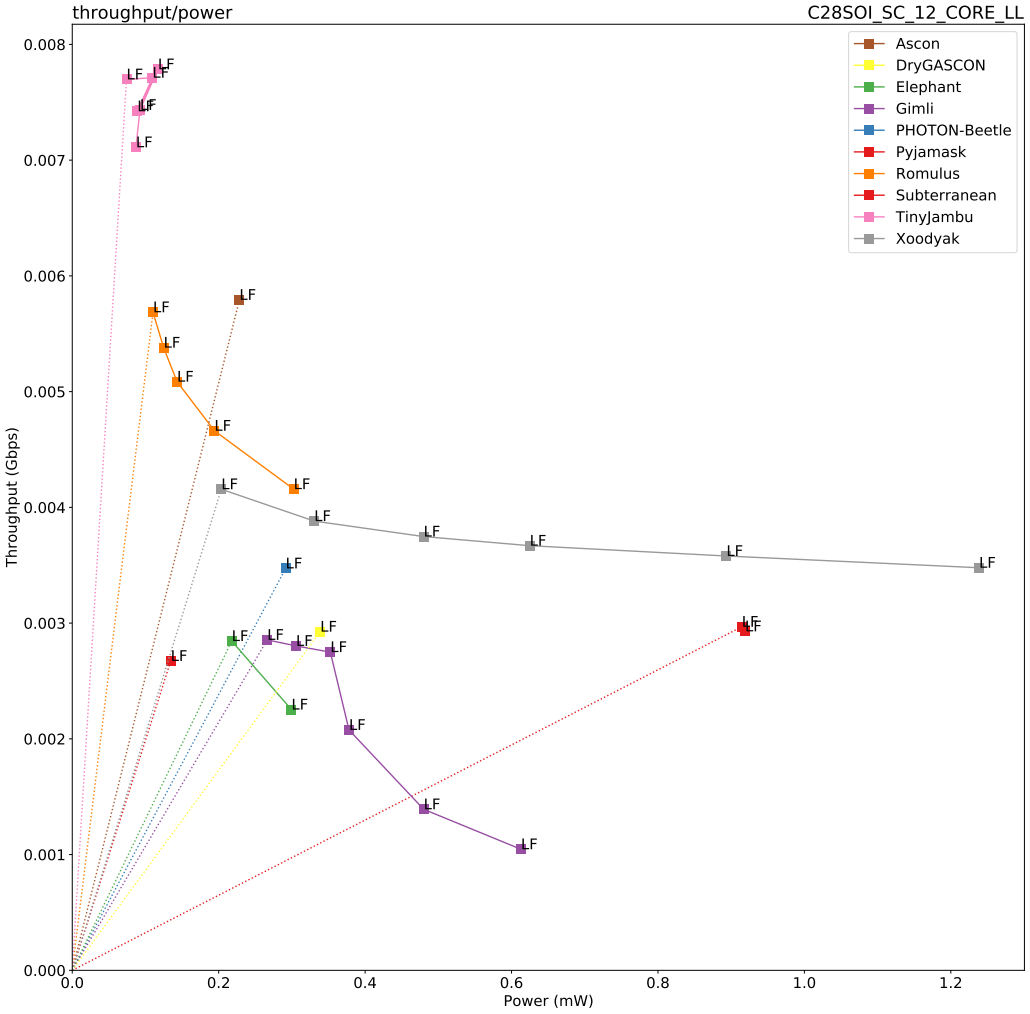

Figure 133: 3 Mbps: Throughput vs. Power for |A| = 1536 bytes on FDSOI 28nm.

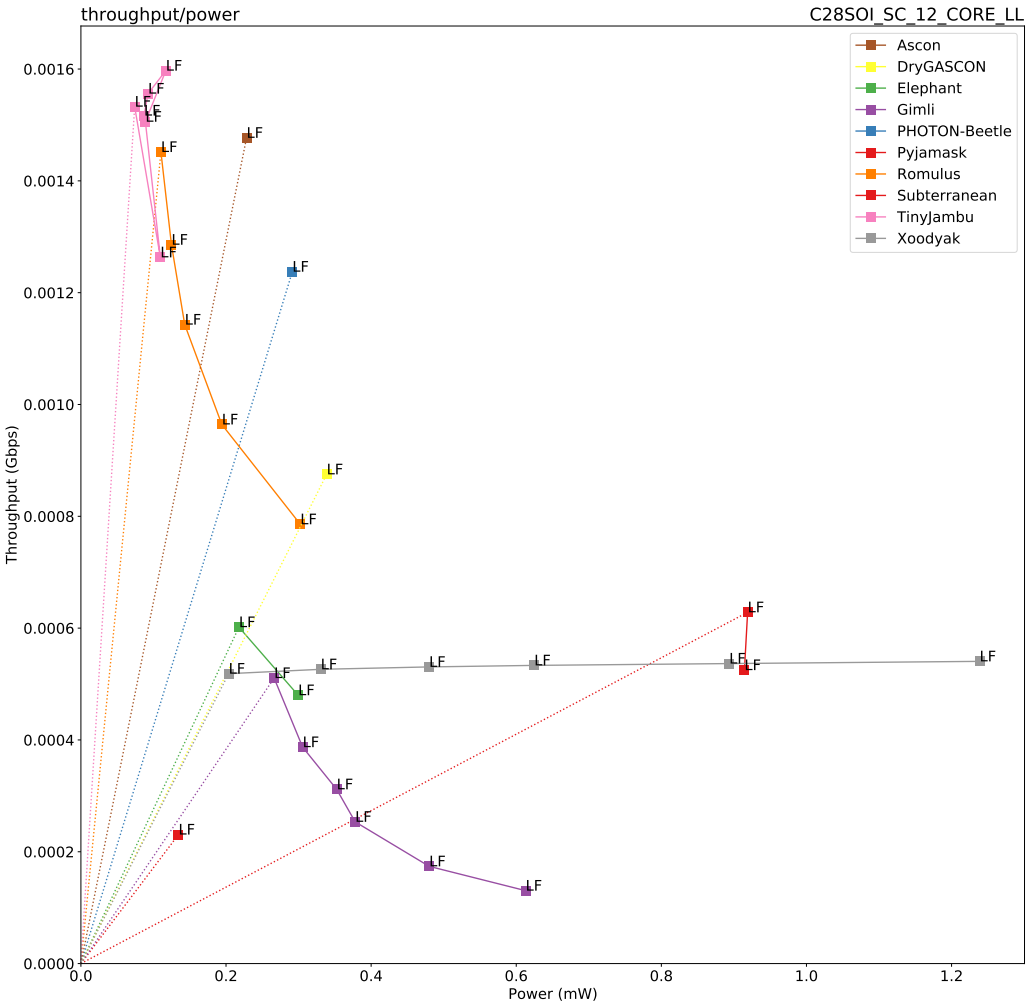

Figure 134: 3 Mbps: Throughput vs. Power for |M| = 16 bytes on FDSOI 28nm.

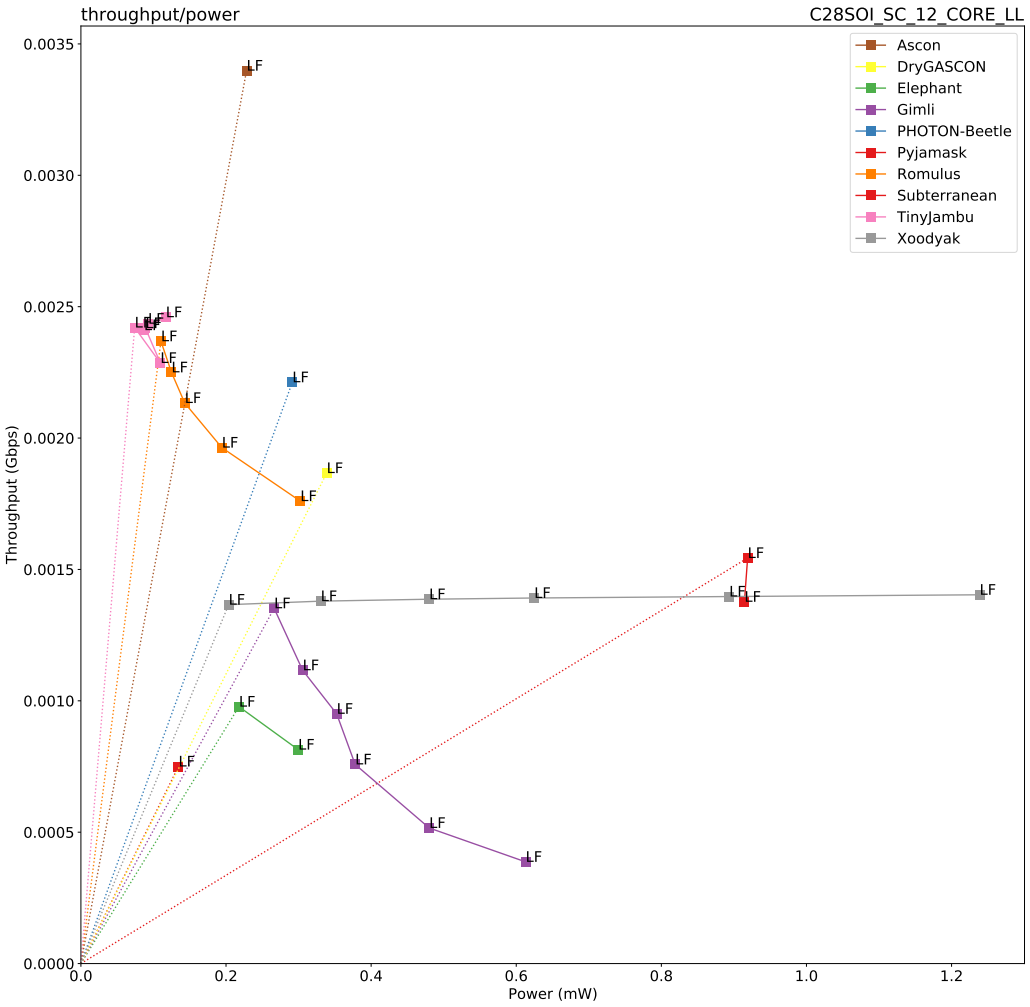

Figure 135: 3 Mbps: Throughput vs. Power for $|M| = 64$ bytes on FDSOI 28nm.

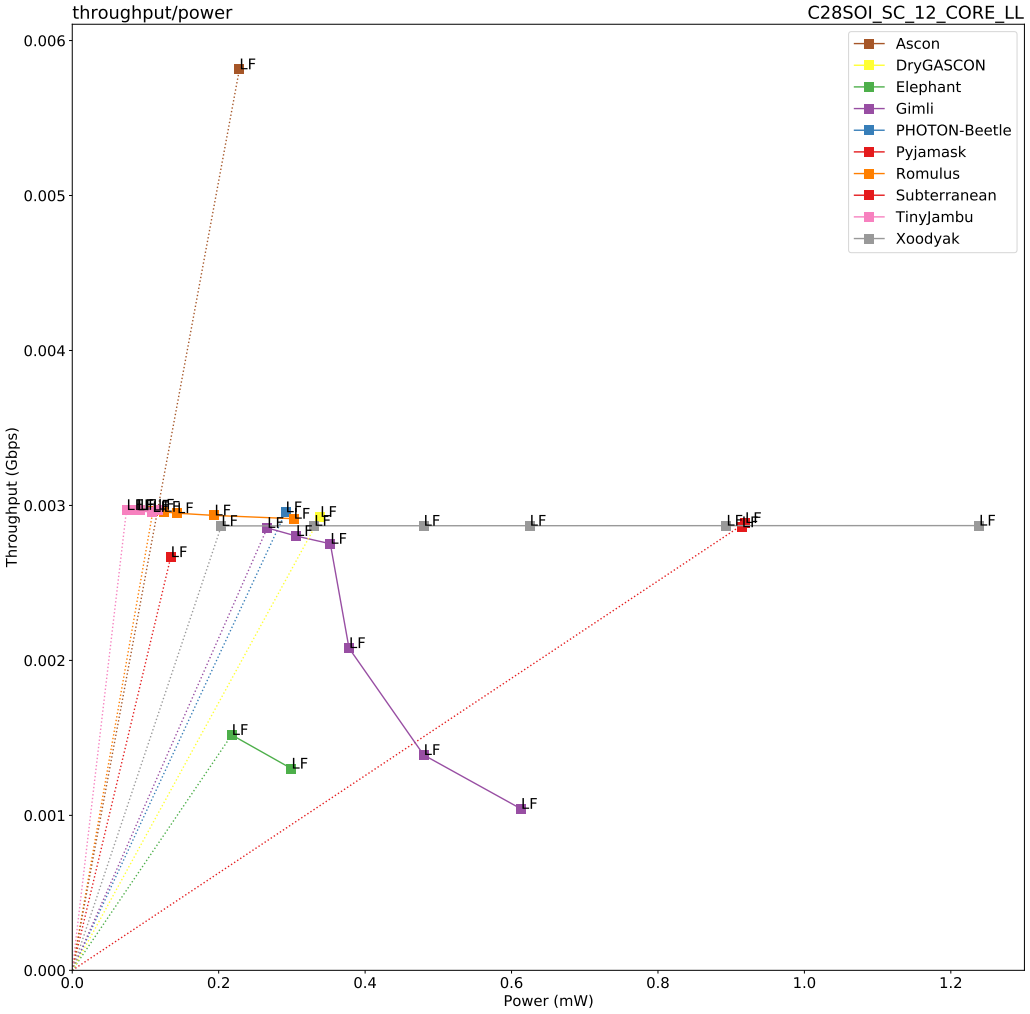

Figure 136: 3 Mbps: Throughput vs. Power for |M| = 1536 bytes on FDSOI 28nm.

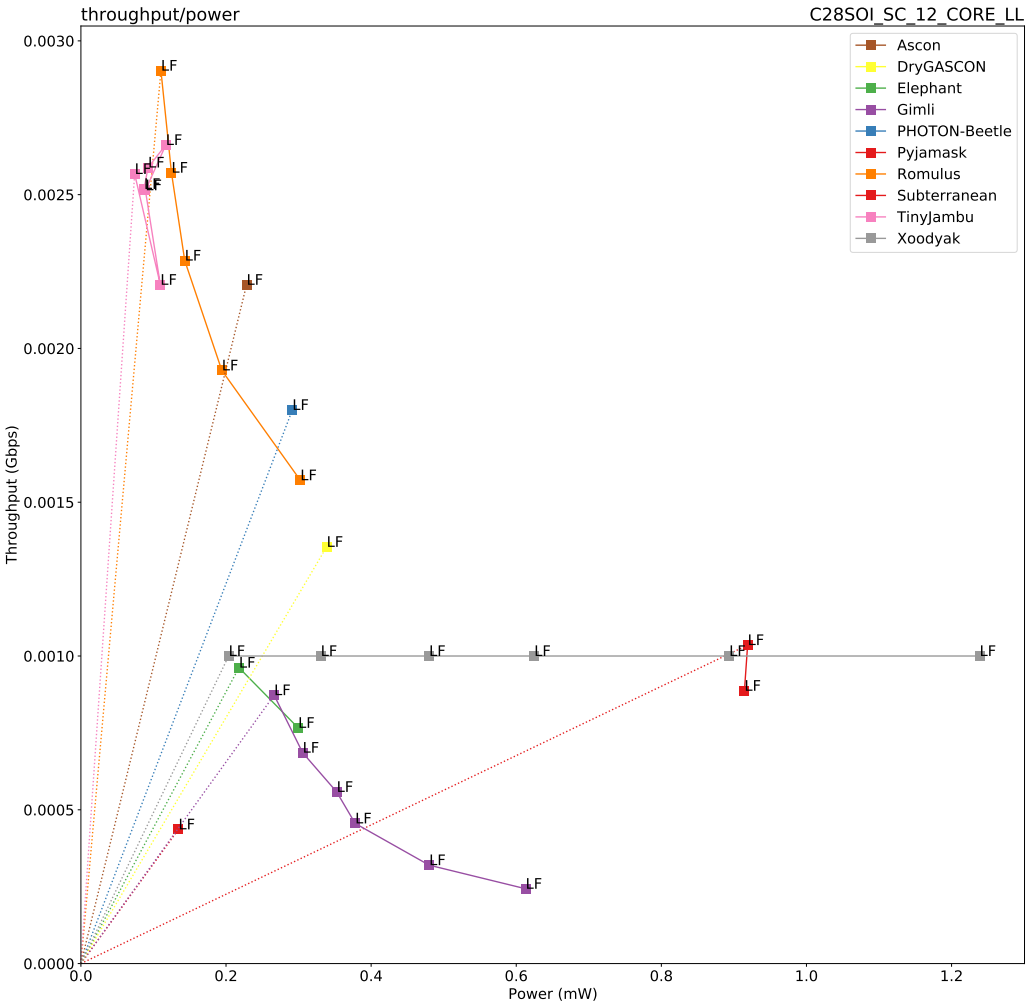

Figure 137: 3 Mbps: Throughput vs. Power for |A| = |M| = 16 bytes on FDSOI 28nm.

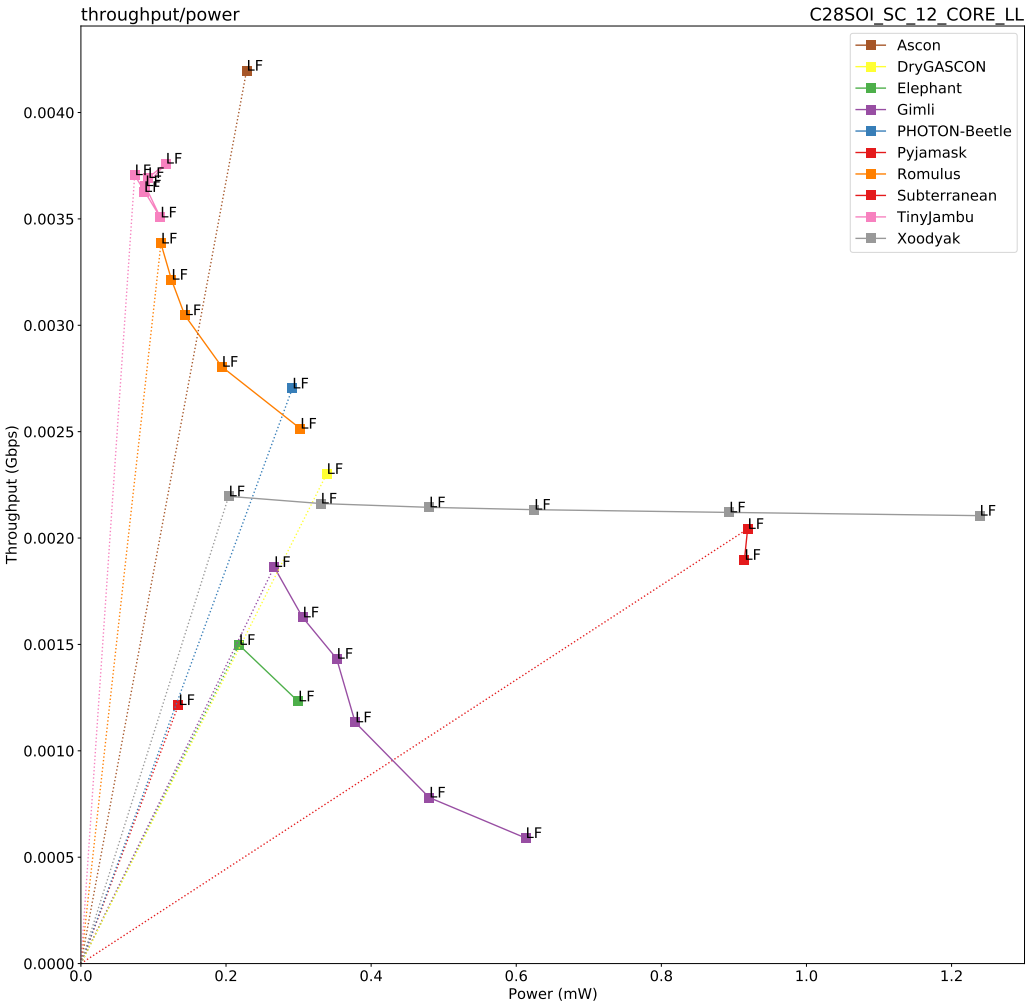

Figure 138: 3 Mbps: Throughput vs. Power for $|A| = |M| = 64$ bytes on FDSOI 28nm.

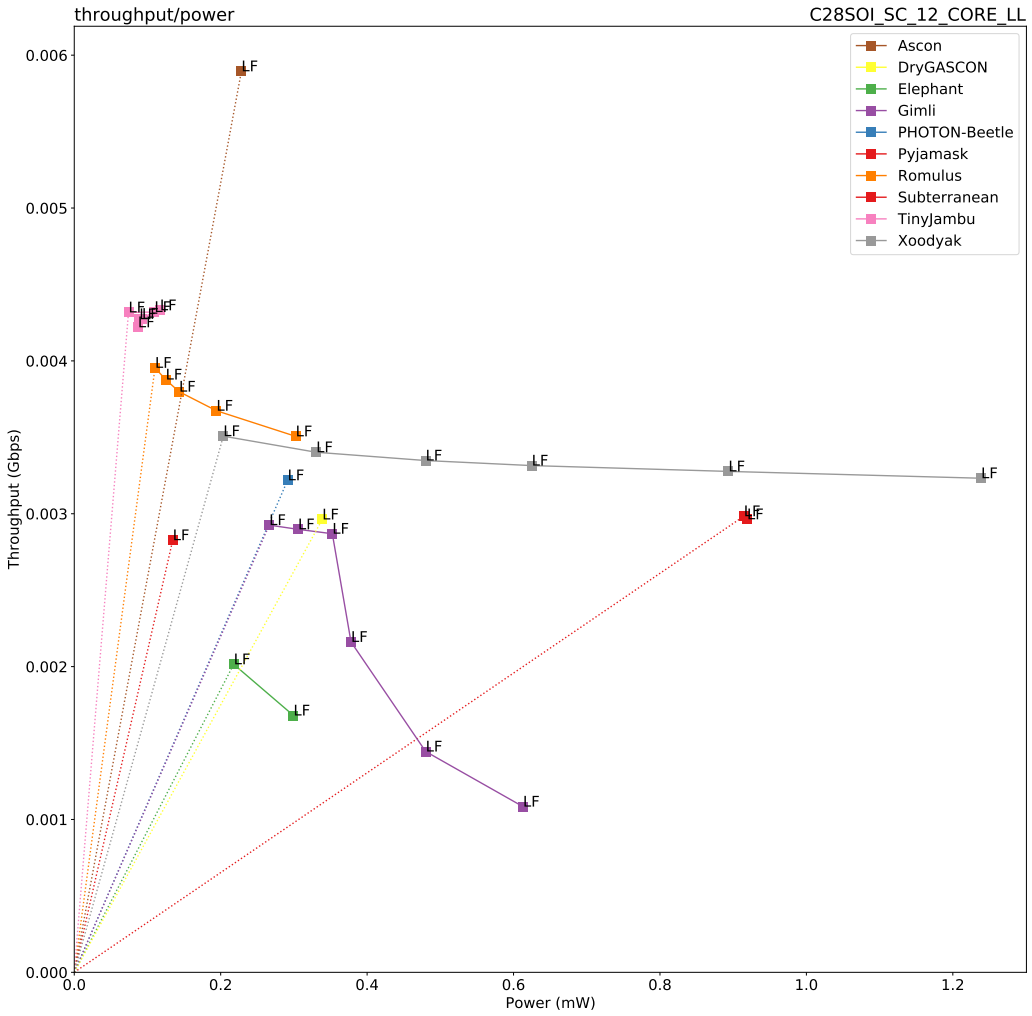

Figure 139: 3 Mbps: Throughput vs. Power for |A| = |M| = 1536 bytes on FDSOI 28nm.