A Comparison of Hardware Side-Channel Countermeasures: Quantitative Analysis of Area Efficiency and Implementation Trade-offs

Xihong Wang
School of Microelectronics, South China Normal University, Guangdong, 528000, China
20233901054@m.scnu.edu.cn

ABSTRACT

Side-channel attacks can easily bypass traditional encryption algorithms by analyzing information such as power consumption and electromagnetic emissions during hardware operation, posing a serious threat to physically accessible cryptographic devices. To defend against such attacks, academia and industry have proposed various hardware protection techniques, including masking, dual-rail logic and randomization. However, the trade-offs among security, area, power consumption and performance vary greatly due to different protection technologies, and designers often lack quantitative standards to choose. In this paper, the surface efficiency of three main hardware protection technologies for side channels is systematically compared, and the ratio between protection strength and hardware cost is used as the main measure. By looking at the representative implementation papers in IEEE and other databases in recent years, and extracting and standardizing the surface (area) data, power consumption, delay and attack resistance levels, this paper constructs a surface efficiency comparison table, and uses radar charts, point cloud charts and bar charts to visually show the advantages and disadvantages of each technology. The results show that masking-based technologies, especially threshold-based implementation and domain-oriented masking, provide the best surface efficiency in high-security scenes. The technology based on dual-track logic provides the highest security, but the cost is high. This paper provides a quantitative reference for selecting protection technologies in different application scenarios, and determines the current research gap and future direction.

Keywords: Side-Channel Attacks; Hardware Protection; Area-Efficiency Comparison; Masking; Dual-Rail Logic; Randomization.

1. INTRODUCTION

With the widespread use of the Internet of Things (IoT) and embedded devices, it is becoming more and more important to worry about the security of encryption chips. Side-channel attacks use physical leaks, such as power consumption, electromagnetic radiation and timing of equipment operation, to effectively find the key [1,2]. Among these attacks, Differential Power Analysis (DPA) is one of the most dangerous methods [1]. Traditional software-based encryption algorithms can hardly resist physical attacks, which makes hardware-level protection an essential choice.

In the past twenty years, researchers have proposed many technologies to protect hardware from side channel attacks. They can be divided into three categories: masking-based technologies (such as Threshold Implementation (TI) and domain-oriented masking (DOM)), logic-based technologies (such as wave dynamic differential logic (WDDL), masking dual-track preload logic (MDPL) and secure three-track logic (STTL)) and random-based technologies (such as clock randomization and randomization) [3-8]. However, there is a great trade-off between the cost (area, power and performance) of implementing these technologies and the level of security they bring. Most of the existing research is mainly about technical principles, and there is little quantitative comparison from the perspective of regional efficiency (that is, the safety benefit per unit hardware cost). This makes engineers have no guidance on encryption and makes them choose in practice [9,10].

This work fills this gap. Through systematic literature review, we choose the classic and representative designs in the above three types of technologies. We extracted data from published papers regarding their area (in GE), power consumption (in μW or mW), frequency/latency, and attack resistance (or TVLA test results) for Application-Specific Integrated Circuit (ASIC) or Field-Programmable Gate Array (FPGA) implementations. We defined an “area-efficiency ratio” metric and conducted a multidimensional comparison. The main contributions of this paper are as follows:

1. A unified framework for comparing area efficiency has been proposed, including definitions and quantification methods for protection strength and hardware overhead.
2. For each of the three mainstream technologies (masking, logic, and randomization), 2-3 classic schemes were selected, and their implementation data at similar process nodes were compiled. Scheme selection followed the following principles: (1) landmark significance; (2) availability of complete ASIC implementation data; (3) coverage of the three mainstream protection approaches. A total of 7 schemes were initially selected, of which 4 provided complete quantification data (see Section 5.2 for details).
3. Radar charts and scatter plots were used to visually illustrate the area efficiency differences among various technologies, and recommendations for selection in different application scenarios were provided.
4. Issues such as data gaps and inconsistent evaluation criteria in current research were identified, and future trends were discussed.

2. BACKGROUND AND RELATED TECHNOLOGIES

2.1 Principles of Side-Channel Attacks

The core of side-channel attacks lies in exploiting the correlation between physical information leaked during the operation of cryptographic devices and intermediate values. Let's take DPA for example. Attackers collect a lot of traces of energy consumption through random complaints. It divides the trajectory into two groups according to key assumptions. Then it calculates the difference between the average trajectories of the two groups. If the assumption is correct, the difference will show a peak at a specific time [1]. First-order (second-order) means that the attacker uses the statistical information from multiple independent leak points at the same time.

2.2 Classification of Hardware Protection Technologies

According to its protection principle, hardware protection technology can be divided into three categories:

Masking-based: Secret data is divided into several random parts. In the calculation process, each part is processed independently, which can ensure that any combination of numbers below the share threshold will not reveal secret information. Typical technologies include threshold implementation (TI), domain-oriented masking (DOM) and low-latency threshold implementation (LLTI). Masking technology provides provable security, but it will produce a lot of surface and random costs.

Logic-based: These technologies use circuit logic design to make power consumption independent of data, such as dual-track and preloaded logic (WDDL, MDPL, STTL). Although these technologies can completely eliminate the dependence on energy consumption in theory, they need strict load balance and lead to extremely high surface area and energy consumption costs.

Randomization-based: These technologies destroy the time or amplitude alignment of energy consumption tracking by inserting random delay, pseudo-operation and shuffling, thus increasing the difficulty of attack. Although the cost of these technologies is low, they do not provide strict security and only increase the cost of attacks.

2.3 Definition of Area Efficiency Metrics

To ensure a fair comparison of different technologies, this paper defines the following area efficiency metrics:

1. Protection strength: The resistance level (the number of DPA orders it can withstand) is used as the primary quantitative metric. For schemes that do not explicitly specify a resistance level, their Test Vector Leakage Assessment (TVLA) results (whether the first-order t-value is less than 4.5) or the security level claimed in the paper are used as a reference.
2. Hardware Overhead: Includes area overhead (normalized to GE, i.e., NAND2-gate equivalent area), power consumption overhead (dynamic power consumption, in μW or mW), and performance overhead (multiplier of latency increase or percentage of frequency reduction).
3. Area Efficiency Ratio: Due to insufficient coverage of power consumption data in existing literature-research indicates that neither DOM nor TI includes power consumption in their discussions [4,11]. This paper adopts a simplified area

efficiency metric: area efficiency = attack resistance order / area overhead (kGE). This metric is practical in area-constrained scenarios and ensures that the four selected schemes can be quantitatively compared.

4. Weighted Composite Score: To provide a more holistic comparison beyond area efficiency alone, we propose a weighted composite score S defined as:

$$S = w\_\{1\} \cdot Sec + w\_\{2\} AreaEff + w\_\{3\} RandEff + w\_\{4\} ImplEase + w\_\{5\} Applic \quad (1)$$

where each dimension is normalized to a 5-point scale (Table 2), and the weights are set as w_1=0.35, w_2=0.30, w_3=0.15, w_4=0.10, w_5=0.10. Security strength receives the highest weight because it is the primary design objective; area efficiency is weighted second as it directly reflects hardware cost in resource-constrained deployments. Randomness, implementation ease, and applicability are assigned lower weights as secondary engineering concerns.

3. CLASSIC SOLUTIONS AND AREA EFFICIENCY ANALYSIS OF THREE TYPES OF PROTECTION TECHNOLOGIES

3.1 Mask-based technologies

Masking techniques are currently the most widely used side-channel countermeasures. We have selected three representative approaches:

3.1.1 Threshold Implementation (TI)

Nikova et al. proposed TI in 2006. By splitting each secret variable into td+1 shares (where t is the algebraic order and d is the security order) and ensuring incompleteness (each component function lacks at least one share), they demonstrated first-order security even in the presence of glitches [3]. Bilgin et al. implemented three TI variants for AES. Among these, the "nimble" scheme reduces the random number requirement per S-box to 32 bits through non-uniform sharing and partial re-masking, with an area of approximately 8.1 kGE (UMC 180 nm) and an encryption time of 246 cycles [11]. Experimental results show that first-order attacks fail within 10 million traces, while second-order attacks require 600,000 traces.

3.1.2 Domain-Oriented Masking (DOM)

The DOM proposed by Gross et al. uses d+1 domains (shares) and achieves scalable masks of arbitrary order by integrating cross-domain product terms after re-sharing them with fresh random numbers [4]. Its first-order AES implementation requires only 7.1 kGE and 18 fresh random bits per S-box evaluation, with an area reduction of approximately 22% compared to similar TI implementations. The second-order implementation (3 shares) has an area of 11.9 kGE and 54 fresh random bits per S-box. DOM demonstrates excellent area efficiency among mask-based schemes, with its advantages becoming particularly pronounced at higher orders.

3.1.3 Low-Latency Threshold Implementation (LLTI)

Arribas et al. proposed LLTI, which significantly reduces latency by decomposing higher-order nonlinear operations into multiple layers of lower-order operations without the need to insert registers between layers [12]. In its AES implementation, the S-box requires only one clock cycle (compared to 3-5 cycles in traditional TI), with an area of 25.8 kGE (45 nm) and a 6.9-fold increase in frequency. However, LLTI incurs relatively high area overhead and is suitable for scenarios where latency is critically important.

3.2 Logic-based technologies

Logic-based techniques eliminate the correlation between power consumption and data at the circuit level; while they offer the highest level of security, they come with significant overhead. Among logic-based techniques, both WDDL and MDPL have been fully implemented in ASICs; this paper focuses on comparing these two approaches. Improved solutions such as STTL are only briefly introduced in the discussion section due to a lack of publicly available quantitative data.

3.2.1 Wave Dynamic Differential Logic (WDDL)

Tiri et al. proposed WDDL, which uses dual-rail architecture and precharging to maintain constant power consumption per cycle [5]. However, WDDL places extremely high demands on routing load balancing, and in practical implementations, power leakage often occurs due to imbalance. Cui Xiaole et al. applied WDDL to the Arithmetic Logic Unit (ALU) of a RISC-V CPU and proposed a random precharge enable technique, reducing power consumption to 42% of that of the original WDDL. However, this resulted in a 15% increase in area and a decrease in the maximum frequency [13].

3.2.2 Masked Dual-Rail Pre-charge Logic (MDPL)

Popp and Mangard proposed MDPL, which uses majority gates and fresh random masks to achieve power randomization without the need for balanced routing [6]. Their AES implementation has an area of 16,421 GE, a power consumption of 122.34 μA at 100 kHz, and a speed of only 59% that of the CMOS version. Although MDPL is resistant to first-order DPA, the power overhead is as high as 17 times. Subsequent low-power modes can reduce power consumption by approximately a factor of 4, but at the cost of security.

3.2.3 Secure Triple-Track Logic (STTL)

Maurine et al. proposed STTL, which uses three-wire encoding (data + validity signal) to completely eliminate the data dependency of timing and power consumption [7]. STTL gates require fewer transistors than SABL (Sense Amplifier Based Logic) gates and are insensitive to load and arrival time imbalances. Simulations show that STTL is effective against DPA attacks, though it has slightly longer propagation delays.

3.3 Randomization techniques

Randomization techniques raise the attack threshold at a low cost by disrupting an attacker's alignment and statistics.

3.3.1 Clock Randomization and Pseudo-Operation Injection

Zhou et al. used four randomly varying clock frequencies in their SHA-3-HMAC SoC, which can prevent power waveforms from being aligned in different encryption operations, thus resisting DPA [14]. The design has a surface area of 493 kμm in 32nm process, the maximum frequency is 300 MHz and the throughput is 17.9 Gbps. However, the specific security forces have not been quantified.

3.3.2 Shuffling

Xu et al. proposed a hardware-friendly hybrid system similar to the Kyber algorithm of Fisher-Yates. By randomly changing the order of operations such as number theory transformation (NTT) and polynomial azimuth multiplication (PWM), they increased the number of oracle needed for CPA attacks from 4k to over 105 [8]. When implemented on FPGA, the system only needs 260 extra slices, and the area-time product (ATP) increases by 8.7%, while maintaining the same number of clock cycles. This method is lightweight and effective, but it is only suitable for algorithms that can randomize the operation order.

4. COMPARATIVE ANALYSIS OF AREA EFFICIENCY

4.1 Data Summary

We extracted typical implementation data for each of the above schemes and normalized them to similar process nodes (180 nm or 45 nm), as shown in Table 1. For ease of comparison, area is standardized to GE (gate-equivalent NAND), power consumption is expressed in dynamic power (μW or mW), and security strength is primarily measured in terms of attack resistance (1st order, 2nd order); TVLA results are noted for some schemes.

Data Collection Methodology: Implementation data in Table 1 were extracted from original publications following a systematic protocol: (1) only post-synthesis or post-layout ASIC results were accepted; FPGA results are marked separately; (2) area figures were converted to NAND2-equivalent gate count using the process-specific conversion factors reported in each paper; (3) security strength was accepted as first-order if either a formal proof or a TVLA result with $|t| < 4.5$ over 10^6 traces was provided. All raw data and source references are traceable to the cited publications. Researchers wishing to reproduce this comparison should refer to the original implementations listed in the References.

Table 1. Summary of Area Efficiency Data for Typical Hardware Side-Channel Protection Solutions.

Technology Category	Representative Proposal	Process	Area (GE)	Power consumption	Frequency/ Latency	Attack Resistance Level	Random number	Area efficiency (/kGE)
Masks: TI	Nimble AES [11]	180nm	8100	NA	246 cycles	1st-order (experimentally verified)	32	0.123
Masks: DOM	1st-order AES [4]	180nm	7100	NA	246 cycles	1st-order (provably secure, TVLA confirmed)	18	0.141
Mask: LLTI	AES [12]	45nm	25800	NA	1-Cycle S-box	1st-order (TVLA verified)	0	0.038
Logic: WDDL	RISC-V ALU [13]	55nm	ALU increased 2.7-fold	5.93→2.49mW	Decrease in frequency	1st-order (design claim)	0	N/A
Logic: MDPL	AES [6]	180nm	16421	122μA@100kHz	10MHz	1st-order (512 traces unsolved)	1 bit per cycle	0.061
Randomization: Shuffling	Kyber [8]	FPGA	+260 slices	NA	Same frequency as the original	Required traces:> 10^5	0	N/A
Randomization: Clock	SHA-3 [14]	32nm	493kμm^2	NA	NA	Non-quantitative assessment (qualitative claims regarding anti-DPA only)	0	N/A

Note: Data is provided for trend reference only under different implementation methods and objectives; precise comparisons require a unified platform.

Note: NA indicates that no specific data was provided in the original text.

Note: Since the original text did not provide quantified data on the security strength of the clock randomization scheme, it is not included in the area efficiency comparison and is provided solely as a reference for implementation overhead.

Note: As the original literature did not provide relevant area data, WDDL and the randomization-based scheme were not included in the area efficiency calculations.

Note: Data in Table 1 most closely approximates a unified comparison under the proposed benchmark (Section 5.3): TI [11], DOM [4], and MDPL [6] all target AES on 180 nm ASIC. Cross-node comparisons (LLTI at 45 nm) are flagged as approximate and normalized by process scaling factor of $\times (180/45)^2 \approx 16$ in area for reference only.

4.2 Area Efficiency Comparison Chart

Based on the above data, we have plotted a radar chart (Figure 1), an area-delay scatter plot (Figure 2), and a bar chart of area efficiency (Figure 3). The radar chart evaluates each technology across five dimensions on a 5-point scale (see Table 2 for scoring criteria). Based on these scores, a weighted composite evaluation is summarized in Table 3. The scatter plot plots normalized area (on a logarithmic scale) on the x-axis and relative delay (with unprotected systems set to 1) on the y-axis. The bar chart directly displays the numerical values for area efficiency.

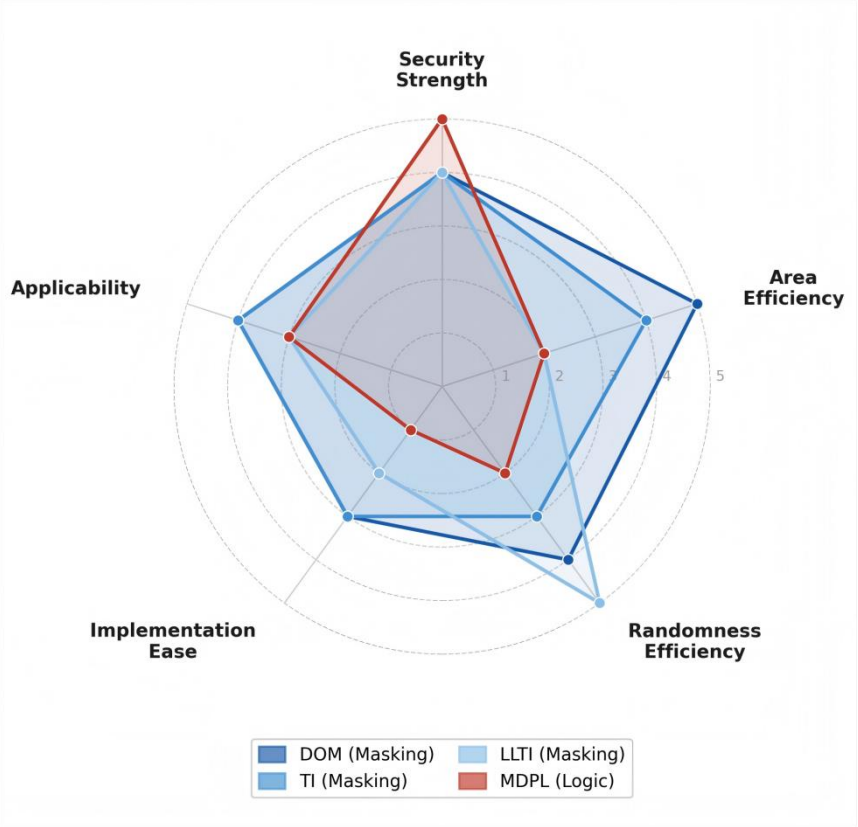

Figure 1. Radar chart comparing four SCA countermeasure schemes across five dimensions (5-point scale; scoring criteria per Table 2).

As shown in Figure 1, the DOM scheme achieves the highest area efficiency at 0.141 per thousand equivalent gates, followed by the TI scheme at 0.123 per thousand equivalent gates. The performance of both is approximately twice that of the MDPL scheme (0.061 per thousand equivalent gates). This result confirms that, under the same security level, a mask strategy adapted to the software achieves a better security-area trade-off compared to dual-rail logic.

Table 2. Five-Point Grading Scale.

Dimension	5 points	3points	1point	Basis for Evaluation
Security strength	Can prove resistance to second-order attacks	Verifiably secure, 1st-order proofs only	Informal security proofs	Published security certificates
Area efficiency	>0.12/kGE	0.06-0.12/kGE	<0.06/kGE	Calculated from Table 1
Efficiency of random number generation	No need for new random bits	A moderate number of randomly generated bits	Each cycle requires a large number of new random bits	Source document data
Ease of implementation	Standard cell flows do not require custom layouts	Requires a small number of custom units	Fully customized units required	Design and Implementation Approach
Scope of Application	Any algorithm and platform	Priority Algorithm Support	Specific to a particular algorithm or platform	Target application scope

Table 3. Weighted composite scores for four representative countermeasure schemes (scoring criteria per Table 2).

Scheme	Sec (×0.35)	Area (×0.30)	Rand (×0.15)	Impl (×0.10)	Appl (×0.10)	Total
DOM	1.40	1.50	0.60	0.30	0.40	4.20
TI	1.40	1.20	0.45	0.30	0.40	3.75
LLTI	1.40	0.60	0.75	0.20	0.30	3.25
MDPL	1.75	0.60	0.30	0.10	0.30	3.05

The composite scores are sensitive to weight selection. The weights adopted here (w_1=0.35 for security, w_2=0.30 for area efficiency) reflect the priority ordering typical of security-critical embedded applications. Designers targeting different deployment scenarios may adjust the weights accordingly-for example, ultra-low-power IoT applications may assign higher weight to area efficiency, while military-grade deployments may prioritize security strength exclusively.

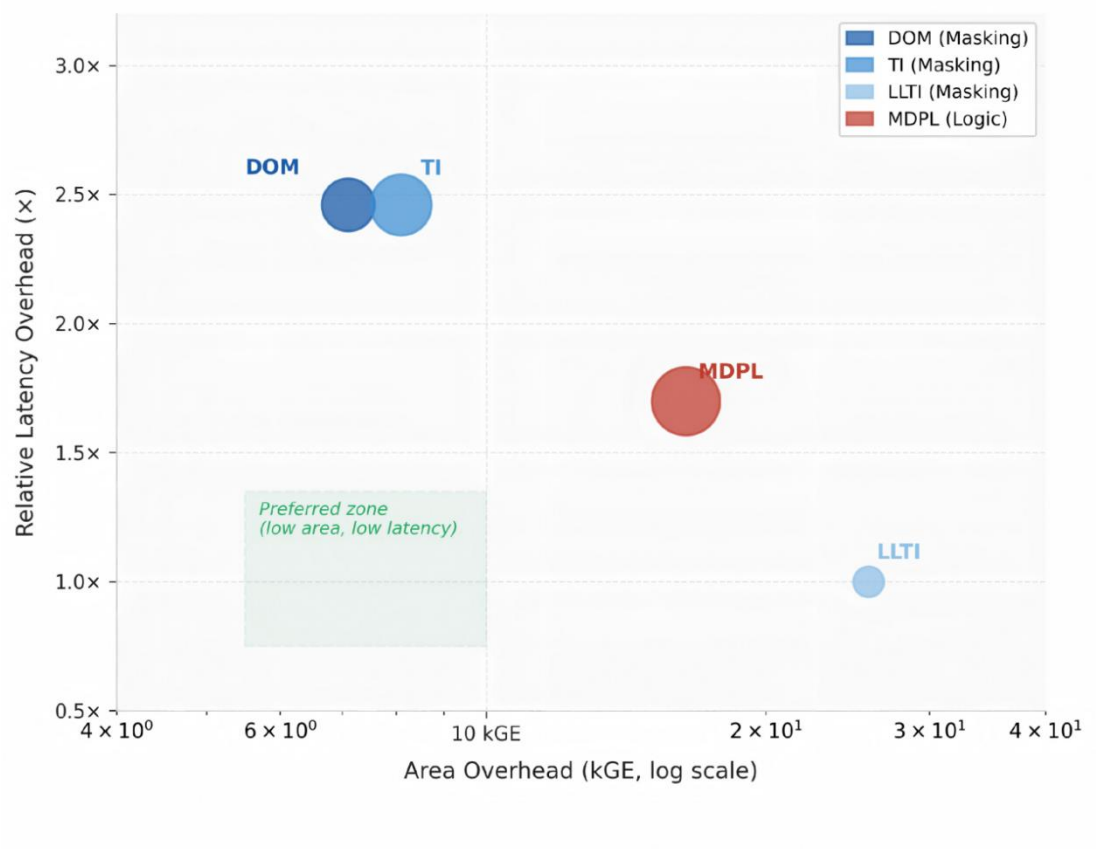

Figure 2. Area overhead (KGE, log scale) vs. latency overhead for four countermeasure schemes; bubble size $\propto$ randomness cost (fresh bits per S-box). Data sourced from Table 1.

Although the LLTI scheme has low randomization overhead (see Figure 2), its area efficiency ranks last at only 0.038 per thousand gates due to the significant increase in the number of gates (26.3 thousand equivalent gates); therefore, it is not suitable for area-constrained applications.

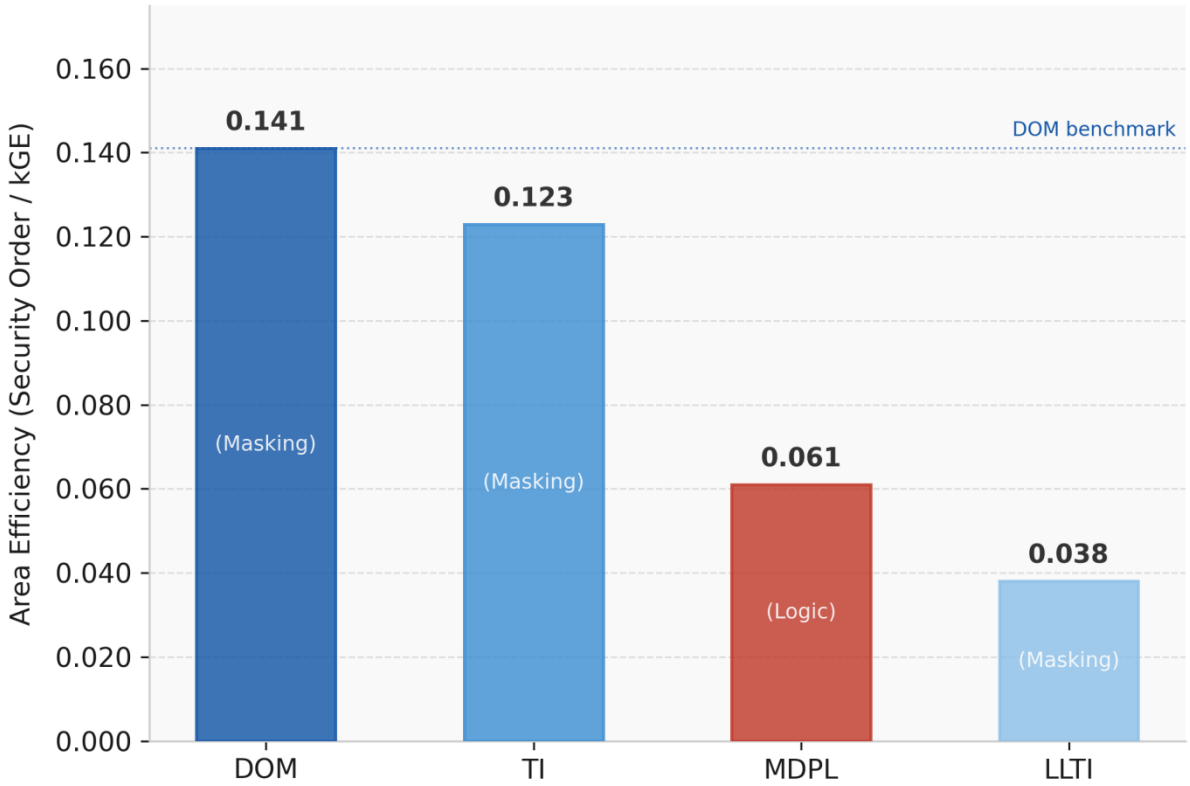

Figure 3. Area efficiency (security order / area overhead in KGE) for four schemes with complete ASIC data. Higher values indicate better efficiency.

4.3 Recommendations for Technology Selection in Different Scenarios

Financial smart cards/high-security chips: Mask-based designs (DOM or TI) are recommended, with priority given to solutions that offer provable security and low random number overhead. The DOM first-order implementation has an area of only 7.1k GE and 18 fresh random bits per S-box evaluation, making it the current optimal choice.

High-Speed Cryptographic Engines (e.g., server and memory encryption): LLTI or shuffling-based variants are recommended. LLTI can complete S-box operations in a single clock cycle but has a larger area; shuffling-based variants are highly effective against post-quantum algorithms such as Kyber and have minimal overhead.

Ultra-low-power IoT sensor: Randomization-based methods (for example, clock randomization) or lightweight masks (for example, partially re-masked TI variants) are more suitable, and high-power logic such as WDDL/MDPL should be avoided.

Extreme physical security (military/anti-intrusion) environment: A hybrid method combining logic-based method (WDDL+back-end replication) and mask can be considered, but it must accept a lot of costs.

5. DISCUSSION

5.1 Limitations of Various Technologies

Mask-based: In high-order (≥ 2nd order) implementation, the surface overhead and random number increase in a quadratic way, and additional registers are needed for sliding robustness, which leads to increased delay. Some solutions (such as TI without random numbers) cannot meet the high-order security requirements.

Based on logic, it is difficult for WDDL/MDPL to achieve complete load balancing on two tracks in the advanced process, which seriously affects the actual security. Although STTL is effective, it lacks the support of automatic design tools, which makes it difficult to adopt it widely.

Randomization-based: It cannot provide verified security, and its effectiveness may decline with the progress of machine learning alignment technology [15].

5.2 Limitations of the current study

Lack of uniform evaluation criteria: The processes, measurement methods and security evaluation indicators (such as TVLA, attack tracking and mutual information) used in different documents are quite different. This makes the comparison between papers difficult.

Lack of data: This review found that only four of the seven candidate schemes initially studied provided complete data to quantify the surface efficiency. Other schemes (WDDL, clock randomization and shuffling) have no standardized surface measurement report. This shows a common problem in this field: researchers usually only share the performance indicators suitable for their own mode, rather than all the parameters of technology implementation. The establishment of a unified indicator reporting standard is still a necessary condition for strict comparison. To this end, we put forward a specific benchmark specification in section 5.3, which can be used as the starting point of community standardization.

Lack of advanced implementation: most protection technologies above the second order are still in the theoretical stage, or have only been verified on a small scale. There is not enough complete implementation data of encryption algorithm.

Insufficient protection against combined attacks: Most researches only focus on DPA. There is little research on the protection ability of combined attacks such as fault injection and electromagnetic analysis.

5.3 Toward a Unified Benchmark Framework

The heterogeneous data identified in Section 5.2 indicate the need for specific benchmark specifications. Based on the implementation conditions of the schemes studied in this paper, we propose the following unified evaluation framework as a reference standard for future scheme comparison.

Common security algorithm and target: AES-128 is recommended as the benchmark password, because it is the most widely implemented algorithm among the three types of countermeasures studied. As the only nonlinear component and the main leakage source, S-box should be used as an evaluation unit. This choice ensures that the cost of surface, delay and randomness is reported in a consistent granularity, and it matches most existing ASIC implementations, including TI [11], DOM [4] and MDPL [6].

General rules of node process and synthesis: We recommend 180nm ASIC process as a starting point, because it is the most frequently mentioned technology in research, and it provides a good reference for security-critical embedded applications. For systems made on other nodes (such as LLTI at 45nm [12]), simple approximations can be used for comparison: the surface change is (180/node) and the frequency change is (node/180). These approximations must be explained. The synthesis should aim at the typical working point of 10 MHz clock frequency, without relaxing the time limit, and use the standard synthesis flow. (e.g., Synopsys Design Compiler or an equivalent open-source alternative such as Yosys with a published cell library).

Common attack model and security metric: Security evaluation should adopt two complementary metrics: (1) TVLA with a significance threshold of $|t| < 4.5$ over a minimum of 10^6 traces, and (2) Minimum Traces to Disclosure (MTD) under a first-order CPA attack using the Hamming weight leakage model. Both metrics should be reported to allow fair comparison between schemes with formal proofs and those with only empirical verification. Higher-order security (second-order and above) should be evaluated using the same methodology applied to each additional share combination.

Common output metrics: Each scheme should report the following implementation parameters in a standardized format: (i) post-synthesis area in KGE (NAND2-equivalent); (ii) dynamic power consumption at 10 MHz in μW; (iii) S-box latency in clock cycles; (iv) fresh random bits required per S-box evaluation; and (v) security level (attack resistance order with verification method). Reporting all five metrics is mandatory; entries not measurable under the available implementation should be explicitly marked as not available with a stated reason, rather than omitted.

Applicability to the present survey: Among the seven schemes surveyed in this paper, TI [11], DOM [4], and MDPL [6] most closely satisfy the above specification: all three target AES on a 180 nm ASIC with first-order CPA evaluation. These

three schemes therefore constitute the most reliable subset for quantitative comparison in Table 1. The remaining schemes deviate from the specification in at least one dimension-process node (LLTI), implementation platform (Shuffling on FPGA), or missing output metrics (WDDL, Clock Randomization)-and are included for qualitative reference only. Applying the proposed framework to a wider set of schemes, including second-order masking implementations and emerging post-quantum countermeasures, remains an important direction for future work.

5.4 Future Trends

Design aided by automation tools: For example, High-Level Synthesis (HLS)-based automatic DOM generation can significantly lower the barrier to entry for secure hardware design [16].

Masks with little or no randomness: Reduce the need for a true random number generator by reusing existing shares (for example, Changing of the Guards technology) [17].

Post-quantum encryption protection: Hardware protection for Kyber and Dilithium algorithms has become a new focus, and technologies such as shuffling and masking need to be optimized for polynomial multiplication.

Unified evaluation platform: the establishment of standardized test platform and public data set (such as SASEBO) helps to compare the efficiency of different protection technologies on an equal footing.

6. CONCLUSION

This paper compares three main hardware-based auxiliary channel attack resistance technologies-masking, logic and randomization from the perspective of surface efficiency. By extracting data about surface, energy consumption, delay and classical safety intensity, the surface efficiency ratio is defined and subjected to multidimensional analysis. The results show that masking-based technology (especially DOM) has achieved the best balance between high security and medium cost, making it suitable for most applications. Logic-based technologies provide the highest level of security, but the high cost limits their use in extreme environments. The method based on randomization is light, but it provides limited security, so it is very suitable for IoT devices with low security requirements. This paper also emphasizes the problems existing in the current research, such as the lack of evaluation standards and advanced implementation, and focuses on the future direction, such as automatic design and post-quantum protection. It is hoped that this work will be a reference for encryption hardware designers to choose technology and provide a benchmark for future research.

REFERENCES

[1] Kocher, P., Jaffe, J., & Jun, B. (1999, August). Differential power analysis. In Annual international cryptology conference (pp. 388-397). Berlin, Heidelberg: Springer Berlin Heidelberg.
[2] Kocher, P. C. (1996, August). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In Annual international cryptology conference (pp. 104-113). Berlin, Heidelberg: Springer Berlin Heidelberg.
[3] Nikova, S., Rechberger, C., & Rijmen, V. (2006, December). Threshold implementations against side-channel attacks and glitches. In International conference on information and communications security (pp. 529-545). Berlin, Heidelberg: Springer Berlin Heidelberg.
[4] Groß, H., Mangard, S., & Korak, T. (2016). Domain-oriented masking: Compact masked hardware implementations with arbitrary protection order. Cryptology ePrint Archive.
[5] Tiri, K., & Verbauwhede, I. (2004, February). A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In Proceedings Design, Automation and Test in Europe Conference and Exhibition (Vol. 1, pp. 246-251). IEEE.
[6] Popp, T., & Mangard, S. (2005, August). Masked dual-rail pre-charge logic: DPA-resistance without routing constraints. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 172-186). Berlin, Heidelberg: Springer Berlin Heidelberg.
[7] Razafindraibe, A., Robert, M., & Maurine, P. (2007, October). Improvement of dual rail logic as a countermeasure against DPA. In 2007 IFIP International Conference on Very LargeScale Integration (pp. 270-275). IEEE.
[8] Xu, D., Wang, K., & Tian, J. (2025). A hardware-friendly shuffling countermeasure against side-channel attacks for kyber. IEEE Transactions on Circuits and Systems II: Express Briefs, 72(3), 504-508.
[9] Wang Pengjun, Zhang Yuejun, &Zhang Xuelong. (2012). A Study on Defense Differential Power Analysis Attacks. Journal of Electronics and Information Technology, 34(11), 2774-2784.(in Chinese)

[10] Curlin, P. S., Heiges, J., Chan, C., & Lehman, T. S. (2025). A survey of hardware-based aes sboxes: area, performance, and security. ACM Computing Surveys, 57(9), 1-37.
[11] Bilgin, B., Gierlichs, B., Nikova, S., Nikov, V., & Rijmen, V. (2015). Trade-offs for threshold implementations illustrated on AES. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 34(7), 1188-1200.
[12] Arribas, V., Zhang, Z., & Nikova, S. (2021). LLTI: Low-latency threshold implementations. IEEE Transactions on Information Forensics and Security, 16, 5108-5123.
[13] Cui Xiaole, Li Xiuyuan, Li Hao, &Zhang Xing. (2023). A Study on Power Suppression Techniques for a Wave Dynamic Differential Logic RISC-V CPU Core. Journal of Electronics and Information Technology, 45, 9. (in Chinese)
[14] Zhou, T., Zhu, Y., Jing, N., Nan, T., Li, W., & Peng, B. (2020, November). Reliable SoC design and implementation of SHA-3-HMAC algorithm with attack protection. In 2020 IEEE International Conference on Smart Cloud (Smart Cloud) (pp. 88-93). IEEE.
[15] Staib, M., & Moradi, A. (2023). Deep learning side-channel collision attack. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(3), 422-444.
[16] Sadhukhan, R., Saha, S., & Mukhopadhyay, D. (2021, December). Shortest path to secured hardware: Domain oriented masking with high-level-synthesis. In 2021 58th ACM/IEEE Design Automation Conference (DAC) (pp. 223-228). IEEE.
[17] Shahmirzadi, A. R., & Moradi, A. (2021). Re-consolidating first-order masking schemes: Nullifying fresh randomness. IACR Transactions on Cryptographic Hardware and Embedded Systems, 305-342.