International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Hybrid Obfuscation with key Based Encryption for Integrated Circuits

T. Pattalu Naidu, A. Kamala Kumari

Abstract*: A new functional encryption method applied for integrated circuit (IC) is proposed in this paper which is called as hybrid obfuscation. The hardware obfuscation or encryption function is a countermeasures act utilized to provide safety of circuit from malware attack and unauthorized entry at the time of manufacture by the distrusted foundries across the world. The purpose of encryption is to design and embed secret keys for achieving functional modifications at the design space itself. Such keys are programmed suddenly inside the ICs when they are obtained from the factory. Since the distrusted factory doesn't approach the key, they can't dispose of the extra components of the chip which doesn't work effectively without the key. By joining existing procedures of obscurity known as fixed obfuscation and dynamic obfuscation, the half and half muddling strategy accomplish the objectives of an encryption function. The investigation of safety efforts proves that the functional encryption enhances the design security as contrasted with existing method. In addition, the proposed method decreases zone overhead by 40% and control overhead by 30% for a key length of 30 bits contrasted with the active obscurity.

***Keywords* : Dynamic and Hybrid Obfuscation, Functional Obfuscation, Hardware Trojan and Security, Logical Encryption.**

I. INTRODUCTION

Most present day electronics businesses are turning in the direction of foundry model requiring the manufacturing outsource of ICs. This opens ICs to become vulnerable, for example, robbery, surplus production, malevolent part inclusion, figuring out and so forth [1], [2]. In such manner, there is a need of expanded significance towards defending electronics circuits by using protection ideas like cryptography based application. One of such procedures is encryption function or equipment muddling of ICs. This method fills in as reverse measures against protected innovation theft and ICs overbuild issues. Functional encryption doesn't carefully pursue the idea of obscurity characterized in programming. But, the objective is attempting to conceal the design functional which corrupts the yields.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
T. Pttalu Naidu *, Research Scholar, Department of Instrument Technology, Andhra University, Visakhapatnam, India. Email: naidu.tamarana1@gmail.com.
Dr. A. Kamala Kumari , Assistant professor, Department of Instrument technology, Andhra university, Visakhapatnam, India. Email:kamala_kumari99@yahoo.co.in

The reverse measure is firmly identified with encryption as mystery keys are consolidated into the analysis before conveying for assembling. Without the mystery key, the endeavor of foundries to privateer or excess produce of the chip are pointless. When the ICs are received from the foundry, the mystery keys are customized on the chips and discharged for sale. This idea is like symmetric key cryptography.

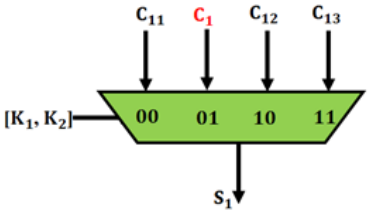
A few ways to deal with functional encryption are discussed in the survey. In light of the perception that ICs which resemble in different may process various capacities and ICs that appear to be unique are figuring similar capacities [3], a method to consecutive rationale obscurity was proposed in [4]. Application of this system on the quick Fourier changes circuit was exhibited in [5], [6]. These procedures are extensively characterized as a fixed encryption class. The fixed obfuscation system experiences the ill-effects of inadequacies like lower security and powerlessness to the device based assaults [7]. A method which expands the design security by using arbitrary and time difference named dynamic obfuscation is proposed in [8]. In this research, the ideas from above plans are utilized to present another system of obfuscation.

The obscurity method proposed gives a 2-phase protection method by consolidating the protection ideas of both fixed and dynamic encryption plans. In particular, it gives concealing function by ruining yields and expanding assault time through arbitrary and time changing attribute. Thus, the cross breed obscurity plan is serving as a device for applications which request a security level among fixed and dynamic encryption. A point by point analysis of the cross breed obscurity conspires with the architecture parameters are discussed. Safety efforts are inferred and usage on equipment IPs is illustrated. An examination of the three encryptions is also provided and fills in as a kind of perspective to pick a method depends on protection versus overhead investigation.

The remainder part of the paper is as pursues. The essential ideas of fixed, dynamic and cross-breed encryptions are presented in Section II. A mode-dependent way to deal with fixed encryption and trigger dependent way to deal with dynamic encryption are introduced in section III and IV. Blend of thoughts from fixed and dynamic schemes to make crossover obfuscation and the analysis of required parts are expounded in Section V. At last, protection examination in view of time to assault and overhead of crossover scheme with regard to region, power and period are discussed in Section VI.

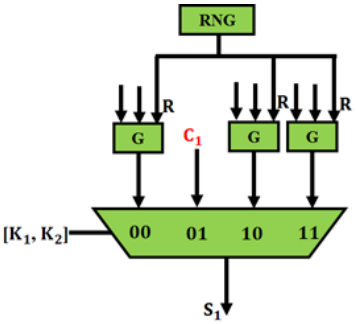
II. HYBRID OBFUSCATION USING TWO-LEVEL OBFUSCATION TECHNIQUE

The obfuscation is achieved by mapping secret keys in the analysis by utilizing exceptional gates termed as key gates. Such key gates may be XOR, NAND, NOR, LUT, multiplexer, etc. When the key source of the framework is wrong, the output will also be wrong for several input keys and true for other input keys. But, the output states are an input based instead of time based processes. So, such type of obfuscation is called as fixed obfuscation. The basic key gate structure for achieve fixed obfuscation is given in Fig. 1 and represented as multiplexer based design.



$[K_1, K_2]$	S_1
00	C_{11}
01	C_1
10	C_{12}
11	C_{13}

Fig. 1.Basic fixed obfuscation structure using MUXs and two key mapping



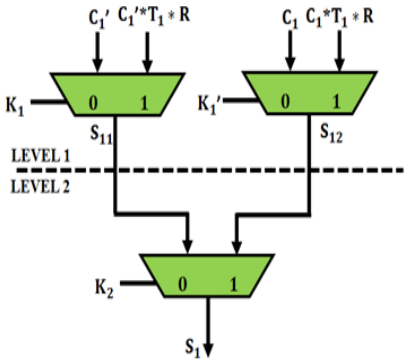
$[K_1, K_2]$	S_1
00	C_1*T_1*R
01	C_1
10	C_1*T_2*R
11	C_1*T_3*R

Fig. 2.Basic dynamic obfuscation structure for arbitrary and time dependent signal and function G

The key bits K1 and K2 are portrayed as the selection symbols of the multiplexers. The input signals of the multiplexers are correct sign (C1) and wrong sign (C11, C12 and C13). Based on the key esteems, the true or wrong signs are chosen at the output S1. In our case, the key worth 01 is true and remaining key esteems are wrong.

Obscurity strength is expanded by increasing period reliance and irregularity in the plan. This kind of muddling was first presented in [8] and named dynamic obscurity. An alteration of the fixed muddling circuit is delineated in Fig. 2. Rather than the wrong key bits choosing wrong sign, the wrong keys are customized to choose progressively varying arbitrary corrupted signals. These signs are received by utilizing an arbitrary number creator as trigger sign T1, T2 and T3, and a blend work G.

Along these lines, the yield is now and then right and once in a while wrong in an arbitrary way. Speculating the right or erroneous key turns into an overwhelming errand and assault period is exponentially expanded. This security improvement was gotten by including a period reliance to the fixed jumbling plan which has not been observed previously. The dynamic muddling plan makes debasement in yield for brief operation time of the circuits and causes the circuit oscillating nevertheless the mystery key is given. But in certain application, it might be alluring in concealing usefulness by tainting the yields similar to the fixed obscurity conspire. Subsequently, a 2-phase method makes adequate defilement in yields when fusing time-differing characteristics and might be a perfect answer in certain application. Such sort of muddling is named cross breed confusion. The plan joins high safety attribute of dynamic muddling with regards to time intricacy of assault and creation of mistaken yields for erroneous key autonomous of fixed jumbling time.



$[K_1, K_2]$	S_1
00	C_1'
01	C_1
10	$C_1'*T_1*R$
11	C_1*T_1*R

Fig. 3.Basic hybrid obfuscation by multiplexer at 2 phase in which phase 1 combines dynamic obfuscation and phase 2 is dedicated for fixed obfuscation

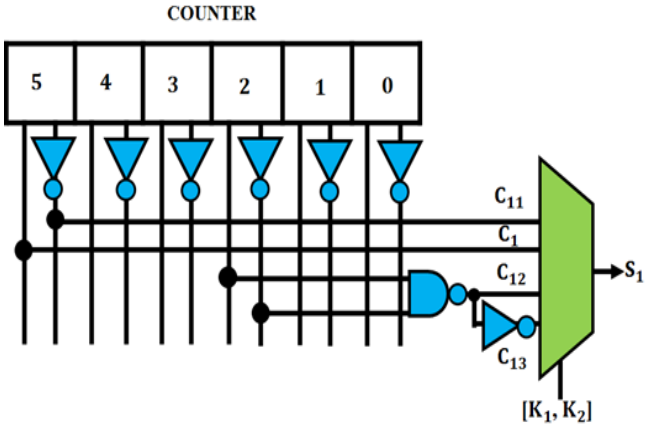


Fig. 4.Control modification to generate mode and key mapping in fixed obfuscation.

Fig. 3 is the fundamental hybrid obfuscation system by multiplexer. 2 keys are projected in each design. Key K1 at phase 1 muddles the sign C1 and its supplement C10 are muddled by trigger dependent powerful obscurity. At phase 2, signs s11 or s12 are chosen depends on K2 muddled utilizing fixed jumbling. The last chosen sign is s1. This circuit functions effectively for key worth 01, progressively for key worth 11 and erroneously for key qualities 01 and 10.

III. FIXED OBFUSCATION BY MODE BASED DESIGN

It is essential to choose the areas in the fixed obscurity in which key-doors are used to create several wrong inward sign mixes. A strategy to fixed obscurity implementation is mode-based methodology as presented in [5]. This approach is described briefly to talk about how the fixed confusion thought can be used to make a cross breed plan. The fixed confusion uses consecutive circuit and chooses the control sign for the key-door inclusion.

In a circuit with memory, control data are acquired from the counter and limited phase machines are critical to the circuit activity. By changing the control data, it is indicated that the structure working in both useful and non-significant mode. The right key chooses an important activity method for the circuits. The remaining keys select the non-important activity method. A straightforward case of control alteration applied to the counter is shown in Fig. 4.

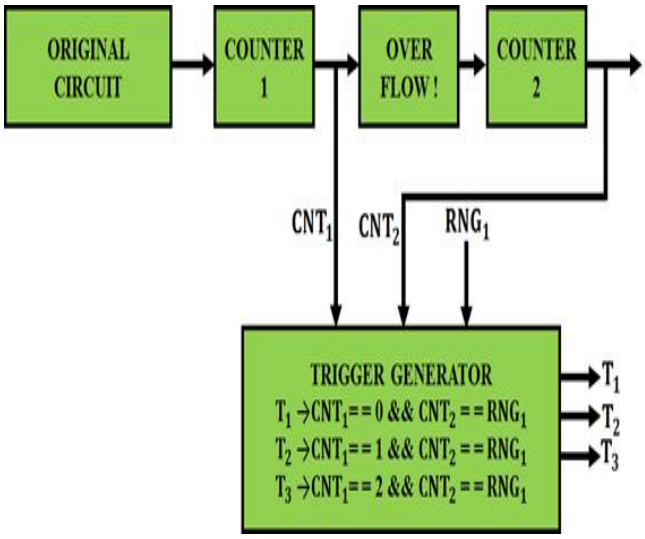


Fig. 5.Trigger creation circuit by counter and arbitrary number generation

The outlined control stream data are extracted from a 6 bit counters. Initially, the right control signal C1 is the invalidation of the counter's MSB bit. Utilizing different bits of the counters with their alterations, signs C11, C12 and C13 are determined. These are then projected as the key door same as figure 1. The utilization of this method on the FFT circuits was exhibited in [5]. The counters in FFT circuits are a 10 bit counter controlling the 1024-point data path.

IV. DYNAMIC OBFUSCATION USING TRIGGER CIRCUITS

From Fig. 2, it is seen that the dynamic jumbling strategy requires additional randomized period-changing trigger signs T1, T2 and T3. The trigger signs are joined with the sign C1 utilizing a blend operator G. In [8], the strategies to produce trigger signs and blend circuits are discussed. The thoughts are portrayed and used it to infer the crossover confusion design. The trigger signs trigger defilement at irregular time interims. Henceforth, it should be time-reliant and arbitrary. The best strategy to accomplish this is to utilize a counter progression with every counter producing enough trigger for the successive counters. Then the arrangement of counter is associated with the first circuit and it is represented in Fig. 5. The piece of the first circuit to which the trigger circuit is associated is the first counter of the planned control circuit. The first counter triggers counter 1 which thusly triggers counter 2, etc. The trigger producing conditions are subject to counter qualities and the output of an arbitrary number generation. Therefore, the objective of acquiring randomized trigger sign is achieved.

The created trigger sign combined with the first counter circuit is given in Fig. 6. It is seen that the trigger sign mix is received via irregular entryways. This guarantees that all the signs are basically design comparative in anticipating discovery and expulsion of the trigger circuit by investigation. Duplicate trigger signs are utilized to accomplish auxiliary comparability for all the data sources. For this structure to be secure, the counter sizes and arbitrary number generation should be painstakingly chosen. Choice subtleties of the counter sizes are exhibited in [8].

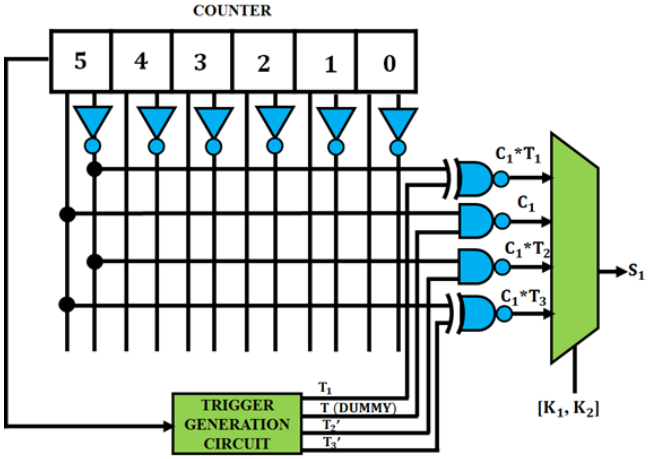


Fig. 6.Trigger circuit and combination gates (T' represents the inversion of trigger signal and it is needed for some combination gates)

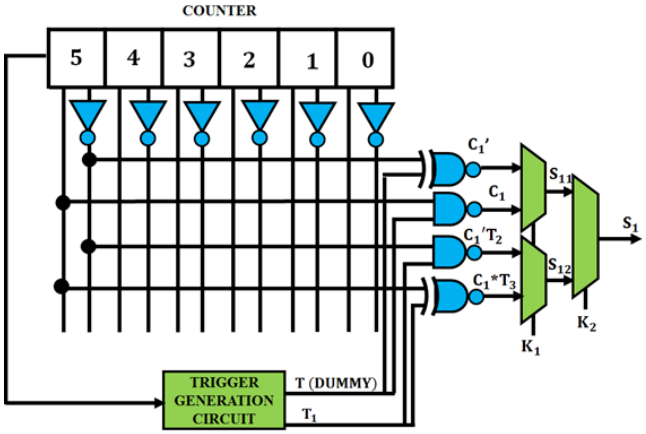


Fig. 7.Small trigger circuit with less number of control signals are needed in hybrid obfuscations.

V. CREATION OF HYBRID OBFUSCATION

The hybrid obfuscation is created by combining thoughts of fixed and dynamic obscurity. The initial phase in this procedure is to supplant every single 4:1 multiplexers mapped to key bit by utilizing the fundamental design of crossover jumbling as appeared in figure 3. In this way, all the 4:1 multiplexers are supplanted with three 2:1 multiplexer. Then, the right and changed control signs are extracted from the control circuits. The signs are defiled by the trigger sign T1 to generate two increasingly mistaken sign mixes. Every signs are fed to the 4:1 multiplexer. This thought is exhibited in Fig. 7. It is to be noted that the quantity of trigger signs required is diminished to 1. Duplicate signs are utilized in the dynamic confusion to make auxiliary similitude for every input of the multiplexer.

Additionally, contrasted with the fixed confusion, just one changed control sign is adequate for cross coupled jumbling.

The half breed jumbling strategy utilizes trigger signs as a part of design procedure. The trigger sign and blend circuit generation are presented in the above segment. Then, the design parameters of the trigger circuit with important adjustments as appropriate to half breed jumbling are presented. Fig 8 shows the mapping of key bit by utilizing the fundamental half and half obscurity structure of figure 3 for a key length of K.

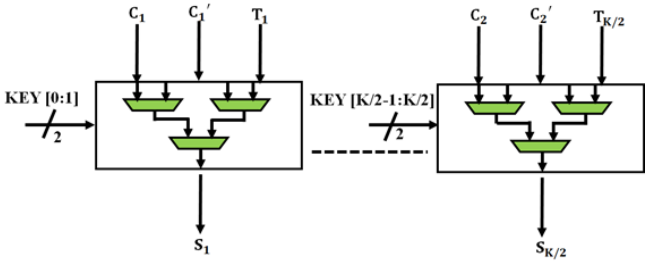


Fig. 8 Mapping structure of hybrid obfuscation to K key bit

From above figure, It is observed that to delineate K bits, K=2 cross coupled obscurities are needed. The obfuscation is made of three 2:1 multiplexer and needs one trigger sign. Subsequently, the absolute quantity of trigger signs needed by this map is K=2T. Likewise note that the trigger sign are chosen by obfuscation for a fraction of the time. With every single key blend, the all out quantity of times a trigger sign is chosen and is equivalent to 2K=2. But due to half and half obscurity, the impact of the trigger sign is just seen in the dynamic jumbled mode. In this manner, successfully, the all out quantity of times a trigger sign chosen is equivalent to 2K=2.

To guarantee non convergence among trigger sign, the counter size of 1 is chosen which may be more prominent or equivalent to the quantity of trigger signs. Thus, the counter size of 1 is equivalent to log2K=2 = log2K□1 log2K. Additionally, to maintain a strategic distance from different key qualities choosing a similar trigger sign, it is guaranteed that the counter size as 2 and irregular numbers generated are more noteworthy than or equivalent to the occasions a trigger sign got chosen. Henceforth, this worth is more noteworthy than or equivalent to log2 (2K=2=2) =K=21, K=2. As the trigger signs are created by counters, the trigger sign are naturally intermittent. The period over which the trigger happens is straightforwardly the adulteration of yields. Henceforth, the trigger time of the trigger signs is a significant variable that influences safety. The trigger time frame is expressed as:

$$\text{Trig\_period} = \text{act\_period} * 2^{\text{size-counter1}} * 2^{\text{size-counter2}}$$

$$= L * 2^{\log 2k} * 2^{k/2}$$

$$= Lk2^{k/2} \quad (1)$$

where activation time frame L is from the base circuit to which the counters are associated.

VI. SECURITY ANALYSIS AND OVERHEAD OF HYBRID OBFUSCATION COMPARED TO FIXED AND DYNAMIC OBFUSCATION

The assailant is suspicious to approach the muddled net list, the function IC from which right I/O sets are produced and information on the confusion method given to the circuit. This is a conventional suspicion utilized in the safety examination of cryptograph calculations. The assignment of an aggressor is to unravel the right key that would be able to open the circuit and duplicate the plan or make different illicit ICs.

Initially the most pessimistic scenario is considered where the assailant lucks out and guesses the right key in the absolute first endeavor. IN fixed confusion, the aggressor can perceive the right key in a period free way by utilizing some info designs and verifying for related yield esteems. Subsequently, an opportunity to assault for this situation is 1. In dynamic obscurity, this worth relies upon the trigger time frame and it was appeared in [8] that the trigger period is equivalent to L K 2K. In cross breed confusion, this worth is diminished to L K 2K=2 as seen from the trigger time frame esteem is already determined. Thus, the half breed confusion gives a low limit between the fixed and dynamic jumbling. Notwithstanding, the worth is as yet corresponding to the key size K even on account of half and half jumbling.

Next we consider a more practical case of the average time to figure out the correct key based on the assumption that on an average, at least half of the key values need to be tried before the correct key is found. This attack time can be divided into two parts. One is for the dynamically obfuscated modes and the other is for the fixed modes. Assuming that the number of key bits used in fixed

Then a progressively down to earth instance is considered where the normal time to make sense of the right key is depending on the supposition that on a normal, at least portion of the key qualities should be attempted before the right key is obtained. This assault time is partitioned into two sections. One is for the dynamic muddled mode and the remaining is for the fixed modes. Expecting that the quantity of keys utilized in fixed muddling is equivalent to the quantity of key bits utilized in powerful confusion, the quantity of modes is equivalent to 2K=2 for dynamic and 2K □2K=2 for fixed. The absolute time to assault is given by equation 2 where t is the time span of the circuit and T is the trigger time frame. The primary term of the whole indicates the beast power assault time for the modes which are progressively jumbled and the second term of the total speaks to modes which are fixed.

$$\text{Time brute\_force (hybrid)} = \sum_{n=1}^{k/2} \binom{k/2}{n} \frac{T}{2} t + (2^k - 2^{k/2})t/2 \quad (2)$$

At last, the assault utilizing data acquired from back figuring is examined. It is expected that the keys are decrypted independently by tapping inside control signals. Such an assault can be focused at two phases. Initially, the assailant can endeavor to unravel the right key K2 at phase 2. When the right key piece makes sense of, either s11 or s12 is identified as the right sign. Consequently, an assailant continues to interpreting the key at phase 1, K1,

to comprehend the correct signs that give right yields for 100 % of the design activity time. The period of assault for key at phase 1 is provided by K1 T. The period of assault for key at phase 2 is provided by a similar expression, however, without the trigger time frame K2 T. In this manner, the absolute time for figuring out assault is provided by equation (3), expecting K1 = K2 = K.

time-reverse_attack (hybrid) = $K_1T + K_2$

$= \frac{K}{2}(T+1)$

(3)

Calculations by utilizing these expressions bring about the estimation of time to assault as arranged in Table 1. It is observed the crossover jumbling isn't as robust as the dynamic obscurity yet offers two degrees of protection. One safety degree is because of the dynamic jumbling and the rest is because of the fixed method of muddling.

For any muddling procedure to be real, the overheads of confusion must be negligible. To begin with, it is considered that the overhead of the extra circuit (trigger producing circuit) is needed for half breed confusion. To produce these qualities, RTL depiction of the trigger circuit is integrated by Design Compiler at an objective recurrence of 100MHz.

Table I. Average Time To Attack Of Hybrid Obfuscation Using Brute-Force And Reverse Engineering For Different Key

KEY SIZE [K1, K2]	BRUTE FORCE ATTACK (CYCLES)	EFFECTIVE KEY SIZE	REVERSE ENG. ATTACK (CYCLES)	EFFECTIVE KEY SIZE
8 [4,4]	5.77 X 10^5	22	542292	22
16 [8,8]	1.68 X 10^8	26	323554	24
[16,16]	9.59 X 10^{12}	46	3.34 X 10^{10}	38

Table II. Gate Counts Of Counter Based Trigger Circuits For Different Key Sizes

KEY SIZE	COUNTER SIZES [CNTD, CNTF]	AREA (UM2)	NUM. OF TRIGGER SIGNALS	GATE COUNT	POWER (MW)	TIMING (NS)
2	(1,1)	54.65	1	24	2.71x 10^{-3}	0.904
4	(2,2)	108.27	2	50	4.45 x10^{-3}	0.778
8	(3,4)	214.82	4	102	6.81x 10^{-3}	0.834
16	(4,8)	368.27	8	178	1.31x 10^{-2}	1.567
32	(5.16)	669.26	16	322	1.66x 10^{-2}	3.014

The implementation result of cross breed obscurity procedure for a real time IP is presented. The circuit for investigation is a 1024 point FFT IP square [9]. The control path of this square comprises of a 10-bit counter is utilized for expansion of obscurity. A similar exploratory arrangement as utilized for producing the past outcomes is utilized for this contextual analysis. Additionally, the strategies of fixed and dynamic confusions are applied to the similar IP blocks. The aftereffects of this test are classified in Table III. From this, it is observed that the overhead of cross breed muddling is between fixed and dynamic confusion. With a view of less quantity of trigger sign and control signs required, both region and power overheads are decreased contrasted with a unique muddling method.

Table III. Comparison Of The Overhead And Time To Attack Of Fixed, Dynamic And Hybrid Obfuscation Using The Controlpath Of A 1024-Point Fft (L=1024)

	Fixed mode of obfuscation			Dynamic mode of obfuscation			Hybrid mode of obfuscation		
Key	Area overhead	Power overhead	Brute-force attack time (cycles)	Area overhead	Power overhead	Brute-force attack time (cycles)	Area overhead	Power overhead	Brute-force attack time (cycles)
4	0.50%	0.11%	8	9.96%	2.06%	688128	5.13%	1.67%	20492
8	0.94%	0.22%	128	17.58%	4.67%	199753728	10.19%	3.06%	$5.6276x10^{05}$
16	1.56%	0.78%	32,768	29.05%	6.45%	1.23 x103	17.20%	5.17%	$1.58x10^{8}$
30	3.23%	1.22%	536,870,912	53.55%	12.41%	3.22 x 10^{21}	31.78%	9.57%	$2.390x10^{12}$

This reduction in overhead includes some significant pitfalls of security reduction and was verified from the security examination. Henceforth, the cross breed muddling plan displays both security and overhead qualities between fixed and dynamic obscurity methods. These patterns are plainly seen from the overhead and security versus key size plotted in below figure.

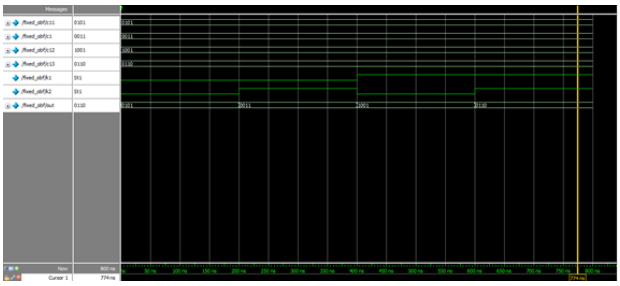


Fig. 9 Time period of fixed obfuscation

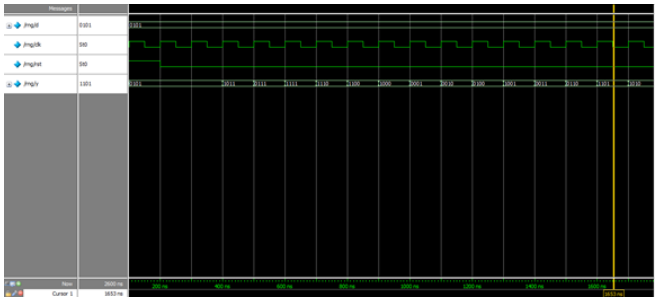


Fig. 10 Time period of dynamic obfuscation

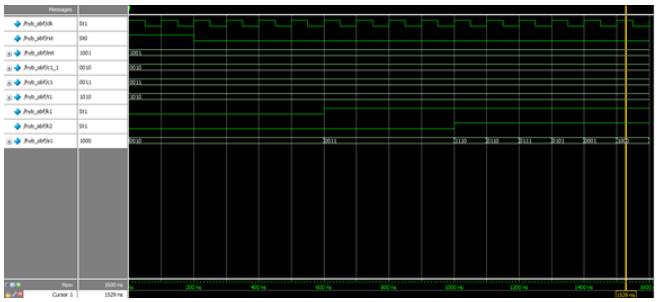


Fig. 11 Time period of hybrid obfuscation

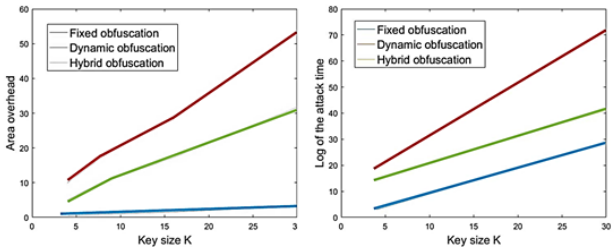


Fig. 12 (a) Overhead vs key size K of fixed, dynamic and hybrid obfuscation

(b) Time to attack vs key size K of fixed, dynamic and hybrid obfuscation

VII. CONCLUSION

A method to equipment obscurity named hybrid muddling which consolidates the safety with regards to concealing operations of circuits by undermining yields and makes the circuits useless only if the right mystery key is fed. It is demonstrated that the most reduced time bound of assault is relative to K=2. The overhead and safety efforts of the half breed confusion were seen to be between fixed and dynamic techniques for obscurity. The future work includes the investigation of assaults on cross breed obscurity utilizing side channel or several solve devices like SAT solver or model checker.

REFERENCES

1. C. H. Kim, and K. K. Parhi, 2018, “Key-Based Dynamic Functional Obfuscation of Integrated Circuits using Sequentially-Triggered Mode-Based Design,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 79–93.
2. Y. Lao, and K. K. Parhi, 2016, “An obfuscated radix-2 real FFT architecture,” in 2015 IEEE International Acoustics, Speech and Signal Processing, IEEE, vol. 7, no. 2, pp. 1056–1060.
3. Y. Xie and A. Srivastava, 2016, “Mitigating sat attack on logic locking,” in International Cryptographic Hardware and Embedded Systems, vol. 3, no. 4, pp. 127–146.
4. F. Koushanfar, and R. Karri, 2016, “A primer on hardware security: Models, methods, and metrics,” Proceedings of the IEEE, vol. 102, no. 8, pp. 1283–1295.
5. K. K. Parhi, 2017, “Verifying equivalence of digital signal processing circuits,” in Signals, Systems and Computers Record of the Forty Sixth Asilomar, pp. 99–103.
6. Y. Lao and K. K. Parhi, 2015, “Obfuscating DSP circuits via high-level transformations,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 23, no. 5, pp. 819–830.
7. S. Koteshwara, C. H. Kim, and K. K. Parhi, 2016, “Mode-based Obfuscation using Control-Flow Modifications,” in Proceedings of the Third Workshop on Cryptography and Security in Computing Systems. ACM, vol. 2, no. 7, pp. 19–24.
8. M. Ayinala, M. Brown, and K. K. Parhi, 2015, “Pipelined parallel FFT architectures via folding transformation,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 20, no. 6, pp. 1068–1081.
9. P. Duhamel, 2014, "Implementation of split-radix FFT algorithms for complex real and real-symmetric data", IEEE Trans. Acoust. Speech Signal Process., vol. 34, no. 2, pp. 285-295.
10. K. K. Parhi, C. Y. Wang, A. P. Brown, 2013, "Synthesis of control circuits in folded pipelined DSP architectures", IEEE J. Solid-State Circuits, vol. 27, no. 1, pp. 29-43.
11. H. Lin, R. Pass, K. Seth, and S. Telang, 2016, “Indistinguishability obfuscation with non-trivial efficiency”, IEEE Transactions on Information Forensics and Security, vol. 13, no. 1, pp. 79–93.
12. T. H. Kim, R. Persaud, and C. Kim, 2014, “Silicon odometer: An on-chip reliability monitor for measuring frequency degradation of digital circuits,” Solid-State Circuits, IEEE Journal of, vol. 43, pp. 874- 880.
13. Yasin M, Mazumdar B, Sinanoglu O, Rajendran J, 2017, “An obfuscated radix-4 real FFT architecture and design”, IEEE design automation, pp. 342–347.
14. K. Seth, and S. Telang, 2017, “Verifying equivalence of digital signal processing circuits,” in Signals, Systems and Computers Record of the Forty Sixth Asilomar, pp. 99–103.
15. S. Suruthi ; M. Arulkumar, 2018, “Pipelined R22SDF, R4SDC FFT architecture via folding transformation”, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 20, no. 6, pp. 1068–1081.

AUTHORS PROFILE

T.Pttalu Naidu is currently pursuing the Ph.D degree with Andhra University college of engineering (A), Andhra University,Visakhapatnam,India. He has teaching experience 8+years.He received M.Tech degree from JNTUK,Kakinada, Andhra Pradesh, India. B.Tech degree in Electronics and Communication Engineering from JNTU,Hyderabad. His current research interests include hardware security (FPGA) and low power VLSI Design

Dr. A. Kamala Kumari is currently working as an Assistant professor, Department of Instrument technology, Andhra university, Visakhapatnam. She has 14+ years of teaching experience.. She received PhD for work on “Design and Development of Mulibeam Antenna for Doppler solar applications from Andhra University in the department of Instrument Technology.she is a member of board of studies in A.U.C.E.A.