ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 7 Issue 3 March 2018, Page No. 23705-23711
Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i3.09

Review on Logic Encryption Strategy Ensuring Key Interdependency

M. Padmaa[1], S. Divyadarshini[2], M. Keerthana[2], T.S. Mohana Parameswari[2], K. Mohana Priya[2]

[1]Professor, Department of ECE, Saranathan college of Engineering, Trichy, Tamil Nadu, India.
[2]Students, Department of ECE, Saranathan College of Engineering, Trichy, Tamil Nadu, India.

Abstract
With the globalization of IC outline flow, numerous fables organizations outsource the creation of their plan to off-site foundries. As these foundries may not generally be believed, it brings about security vulnerabilities and dangers, for example, forging, IP theft, figuring out, overbuilding and Hardware Trojans. Logic encryption has developed to be a potential answer for secure the plan against these dangers. It presents some additional equipment (key-gates) into the plan to conceal the usefulness from unapproved clients, utilizing security keys. The areas of addition of key-gates decide the nature of the security gave by the subsequent plan. In this paper, we examined pros and cons of few papers and propose a productive technique to defeat the IP theft.

Keywords – Security, Reverse engineering, IP Piracy, Key – interdependency, Logic encryption

Introduction

Due to the colossal cost of setting up and keeping up a foundry, numerous Integrated Circuit organizations work fables. The organizations outsource their outlines to outer foundries for assembling. Nonetheless, these foundries may not generally be trusted and here and there are the potential wellsprings of security dangers, for example, Intellectual Property (IP) robbery, figuring out, overbuilding and equipment Trojans. As the foundry may have noxious client, they may figure out the plan and claim the responsibility for IP. They may embed pernicious circuits into the outline or may even finished deliver ICs and illicitly offer the extra chips. In this manner, securing the outline and ensuring the IP has turned into a noteworthy test for the IC originators, particularly for organizations with no creation office.

At the point when the creator sends the encoded configuration to the foundry, he doesn't stack the secret enter into this memory as it can be recouped by an assailant in the foundry. The foundry produces the IC and returns them to the architect. The planner at that point stacks the secret enter into the carefully designed memory and makes the ICs practical. To keep a client from perusing out the secret key from the memory, the creator evacuates read/compose access to this memory by extinguishing the wires in the read/compose circuit. Besides, to keep an assailant from perusing out the substance of the memory, it is intended to be carefully designed.

We are taking three papers titled,

- A New Logic Encryption Strategy Ensuring Key Interdependency
- Fault Analysis Based Logic Encryption
- On Improving the Security of Logic Locking

A New Logic Encryption Strategy Ensuring Key Interdependency

Different Logic encryption procedures utilize OR/XNOR gates AND/OR gates, multiplexers, or some of the time a combination of every one of these components to encode the outline. The XOR/XNOR based encryption method has been proposed in EPIC (Ending Piracy of Integrated Circuits). It embeds XOR/XNOR gates (key gates) arbitrarily into the outline. One contribution of the XOR/XNOR gate is associated with some inner line of the circuit, while the other info fills in as a key-input. These XOR/XNOR gates are designed as supports after applying right keys, else upset the line prompting incorrectly yield for invalid keys. To beguile an attacker from speculating the right keys, a portion of the XOR gates are supplanted by XNOR

and inverters and the other way around. To guarantee high yield corruption for invalid keys, a fault analysis based key-gates [3] area determination approach has been proposed by the creators.

Fault analysis based key-gate location selection

This strategy utilizes three essential phenomena, Fault excitation, fault propagation and fault masking of IC testing to choose the locations to embed key-gates. Use of inaccurate key is considered practically equivalent to the excitation of either a stuck-at-0 (sa-0) or stuck-at-1 (s-a-1) fault. This strategy distinguishes several locations in the circuit, where if any fault happens [3] (either s-a-0or s-a-1), it proliferates to the yield and defiles a maximum number of yield bits for the majority of the connected info patterns. These are the potential areas to embed key-gates. Advantages: This strategy encourages the originator to controllably degenerate the yields for erroneous keys. It tries to accomplish a half Hamming separation between the right yield and the debased yield to amplify uncertainty for an attacker. Disadvantages: Path Sensitization Attack: Both arbitrary and fault investigation based key-gates inclusions are defenseless against way refinement attack. An assailant can remove the keys with the assistance of one useful IC (can be purchased from the market) and a scrambled net list.

Strong Logic Encryption

To relieve way refinement attack, Yasin et al. [2] has proposed to embed the key-gates in chose areas to increase the interference between the key-gates. Their proposed strong logic encryption technique shapes an inner circle of key-gates, where every one of the hubs (key-gates) meddles with each other. The extent of the faction is the length of the keys. The goal is to maximize the faction size to expand the key-length. Advantages: Strong logic encryption is secured from paths sensitization attack. No key-gates can be sharpened to the output without controlling alternate keys. This expands the attacker's effort to separate the key bits. Disadvantages: Searching for an expansive number of interfering key areas is to a great degree troublesome and is totally dependent on the circuit topology. Brute force attack may be a potential attack for such a plan secured with less number of keys. Additionally, as the key-gates are put with an objective to increment the inner circle measure, it doesn't generally ensure high yield defilement for wrong keys. Decreased Hamming distance amongst right and defiled yield may ease the task of an assailant to anticipate the right key.

In their proposed work, another logic encryption system with exceedingly subordinate key structure is displayed. It is partitioned into two phases.

Phase 1

To begin with, they proposed a modified fault analysis based logic encryption method, which chooses a majority share of the key-gates areas in light of the fault effect of each gates exhibit in the circuit. The yield of the gates with the most elevated fault effect is chosen as the area of key-gates position, if it isn't an information or yield of effectively put key-gates. Whatever remains of the key-gates are embedded to keep the way sharpening of the effectively put key-gates. To confine the attack, they check the information cone of dependency (ICOD) of line m. On the off chance that no key-gates is available in the ICOD [1] of a particular line, they embedded a key-gates before that line. The net list is re-combined after the addition of each key-gates. For every cycle of key-gates inclusion, the key-gates embedded at past emphases are given irregular inaccurate keys to copy numerous stuck to fault situations for all the beforehand embedded key-gates.

Phase 2

The proposed logic encryption system keeps the way sharpening attack. Be that as it may, it doesn't ensure high impedance among the keys. Figure 1 demonstrates the circuit diagram of the key-dependency block [1] with 16 key-inputs. It comprises of XOR and XNOR gates associated in three phases. This circuit can be summed up for any number of key-inputs. For a circuit with N number of key sources of info, PK is ($\forall i = 0 \rightarrow N-1$) are the essential key-contributions to the key-dependency square and SK is ($\forall i = 0 \rightarrow N-1$) are the auxiliary keys out of the piece, which are really sustained to the key-gates of the encoded circuit.

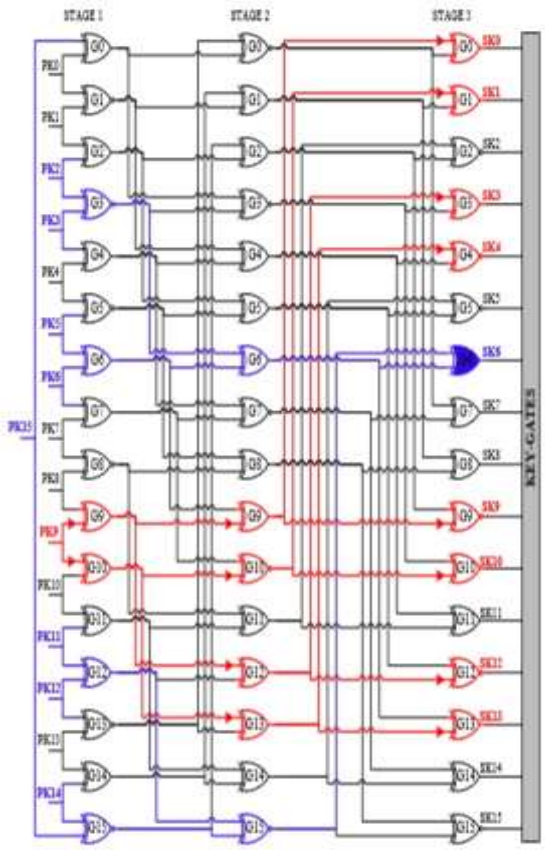

Fig. 1 Key-dependency block with 16-bit key.

Inference

In this work, they have proposed a modified logic encryption approach, which embeds greater part of the key-gates in light of fault examination, to guarantee high yield defilement for invalid keys. This boosts the equivocalness for an assailant to figure the right key by watching the yield. Whatever is left of the key-gates are embedded to guarantee that none of the key-gates can be sharpened to the yield. They likewise have acquainted a key-dependency block with increment the dependency between the key-inputs, which expands an attacker's push to uncover the keys.

2.6 Advantages

As the authors encrypt the design with a sufficiently large number of keys, a brute-force attack is also practically impossible. The evaluation of their proposed logic encryption technique against several security threats like path sensitization attack, hill-climbing attack etc. shows that it is secured from most of the proposed attacks.

2.7 Drawbacks:

Recently, a SAT-based attack has been proposed which can extricate the keys utilizing an efficient SAT solver. Be that as it may, it has been connected just on littler circuits. The unpredictability of SAT-based attack [5] increments with the span of the circuit and key-length. As our key size is substantial and the joining of key-dependency piece includes additional multifaceted nature into the outline, they trust that applying SAT-construct attack in light of bigger circuits, encoded with sufficiently extensive keys utilizing their strategy, is difficult. The future course of this work is to build up a formal verification of protection of our technique against SAT-based attack to approve our claim.

Fault Analysis Based Logic Encryption

Logic Encryption

Logic encryption conceals the usefulness and the execution of a plan by embedding some extra gates called enters gates into the first outline. All together for the plan to display its right usefulness (create revise yields), the legitimate key must be provided to the scrambled outline. After applying a wrong key, the scrambled plan will show a wrong usefulness (deliver wrong yields).

FaultAnalysis using Logic Encryption

The procedure to encode a plan utilizing key-gates (e.g., XOR/XNOR) such that any wrong key causes a wrong yield. This is like the circumstance where a circuit creates a wrong yield when it has a fault that has been energized and spread to the yields.

Fault excitation

Utilization of a wrong key can be related with the enactment of a fault. For a wrong key, either a stuck– at– 0 (s– a– 0) or stuck– at– 1 (s– a– 1) fault will get energized when key-gates are utilized for encryption. Consider the circuit encoded with one XOR gates(E1).

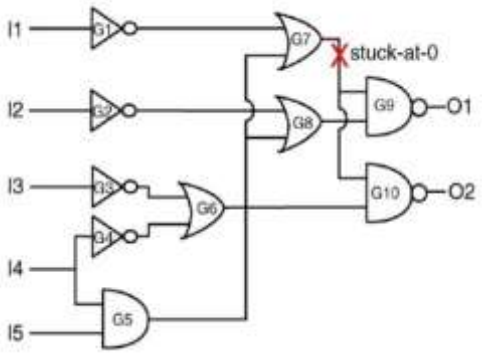

Fig. 2 Fault Excitation

In the fig. 2, E1 is the key-gate. On the off chance that a wrong key is connected to the circuit, the estimation of net B is the negated estimation of net A. This is the same as energizing a s-a-0 or s-a-1 fault at the yield of G7. It is noticed that s-a-0 (s-a-

1) fault enactment can be credited to the situation where the net being referred to is supposed to yield an estimation of 1 (0) amid the utilitarian mode of task.

Fault propagation

Not all wrong keys can degenerate the output as the impacts of a wrong key might be hindered for some of the information designs. This is like the situation where not all input examples can proliferate the impact of a fault to the output.

Consider the circuit appeared in Fig.3. Let a wrong key be connected to the circuit. For the information design 00000, an s– a– 0 fault gets energized at the yield of E1 and propagates to the two yields. The incentive at the yield of E1 is 0 rather than 1, and the yield is 11 rather than 00. For the info design 01110, despite the fact that the s– a– 0 fault gets energized at the yield of E1, the yield is 11, which is the correct yield, as the fault impacts have been blocked. Since not all information designs ensure the non-controlling values on the fault spread way, a wrong key won't generally degenerate the yield.

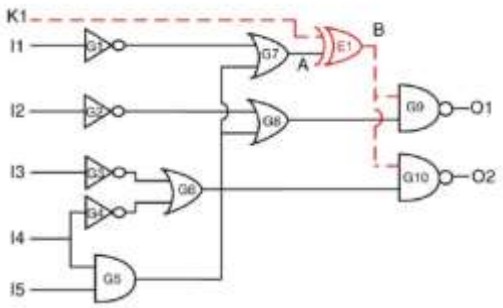

Fig. 3 Fault Propagation

Fault masking

Inserting a solitary key-gates and applying a wrong key is proportional to energizing a solitary stuck-at fault. Likewise, embedding numerous key gates and applying a wrong key is equal to all the while energizing various stuck-at faults. However, when different deficiencies are energized, they may veil each other. Thus in logic encryption, when multiple key-gates are embedded, the impact of one key-gates might mask the impact of other key gates. Consider the circuit in fig 4. When the key bits are 000, the right utilitarian yield is 00 for the input design 00000. In any case, if the key bits are 111 (wrong key), the impact presented by the XOR gates, E1, is conceal by the XOR gates E2 and E3. Therefore, the plan produces the revise yield, 00. Like fault covering in IC testing, the impact of one XOR gate is concealed by the impact of the other two XOR gates.

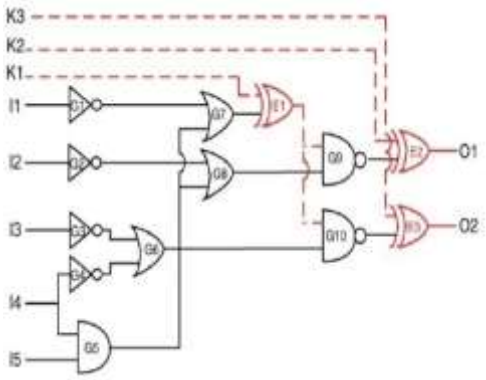

Fig. 4 Fault Masking

Despite the fact that the above situation compares to masking the impacts of shortcomings (key-gates), the average situation in IC testing happens when the impacts of a similar fault counterbalance [3] due to re-concurrent fan structures Fault concealing occurs despite the single fault presumption in IC testing. Objective is to embed the key-gates with the end goal that a wrong key will affect 50% of the yields for any info design. As far as fault simulation, this objective can be expressed as finding an arrangement of faults which together will influence half of the yields for a wrong key on applying an information design.

Inference

An architect can embed key-gates only at the outputs to account for fault excitation, propagation, and masking. Be that as it may, in such additions key-gates will influence just a single yield bit. The fault analysis-based insertion technique makes use of the fan-out structures to recognize the best area inside the circuit to such an extent that various yields are influenced by a solitary key-gate. Thus, each output-bit will not be directly correlated with a key-piece.

Advantages

On increasing the key size will make it harder for an assailant to recover the secret key. Thus, it breaks the savage power attack. It can be seen that fault-analysis based logic encryption results in more uncertainty for an attacker than arbitrary inclusion of gates. Indeed, even by expulsion of key gates from the scrambled net list, the assailant can't prompt the finding of secret key.

Drawbacks

In this work, just a single key-gate is embedded per emphasis. Such addition might be computationally

costly for huge outlines. Path Sensitization Attack: Both irregular and fault examination based key-gate inclusions are defenseless against way sharpening attack. An attacker can extricate the keys with the assistance of one practical IC (can be purchased from the market) and a scrambled net list.

On Improving the Security of Logic Locking

Logic locking conceals the usefulness and the implementation of a plan by embedding extra gates into the original outline. All together for the outline to show its correct functionality (i.e. produces redress yields), a substantial key has to be provided to the bolted plan. The gates embedded for locking are the key-gates. After applying a wrong key, the locked configuration will display a wrong usefulness (i.e. deliver wrong yields). The creators abuse the vulnerabilities of existing logic locking strategies and propose an attack against such techniques. In the proposed attack, with help of a bolted net list and a practical IC, an assailant generates and applies particular info designs, watches the yields for these examples, and translates the secret key the authors present a security metric that aides a logic locking technique in embedding key-gates, expanding attacker's exertion to break it. In light of this new metric, they build up a solid logic locking method. They at that point enhance upon the proposed logic locking strategy by building up a judicious first key-gates determination procedure. They decrease the execution time of our proposed calculation by developing necessary conditions for pair wise security of key-gates and eliminating pointless tests for security. They likewise assess the security of proposed logic locking techniques against two as of late proposed attacks: the hill climbing search attack and the SAT-based attack. They likewise propose another countermeasure against the SAT-based Attacks.

Strong Logic Locking

Strong logic locking depends on embedding key-gates with complex impedances among them Interference chart. To embed key-gates, they shape an impedance diagram of key gates.

Interference graph

In Fig. 5, every hub speaks to a key-gates and an edge interfaces two hubs, if two gates meddle. Confined key-gates are spoken to with secluded hubs. A run of key-gates is meant by a solitary hub. Non-alterable key-gates are associated with non-changeable edges; concurrently mutable key-gates are associated with variable edges. Sequentially mutable key-gates are associated by two edges; a non-mutable edge emerges from the key-gates that is non-variable and a changeable edge emerges from the key-gates that is impermanent.

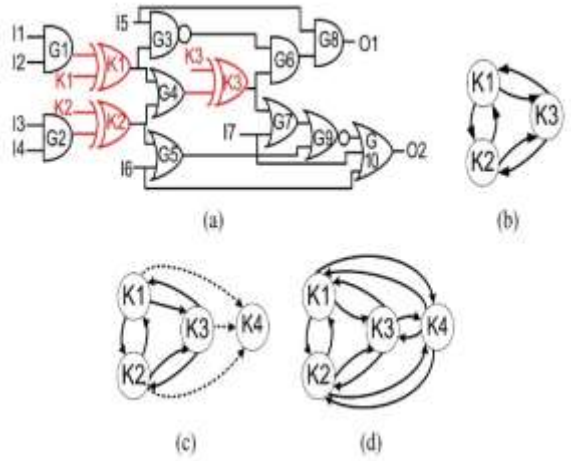

Fig.5 (a) Example circuit with three key-gates. (b) Interference graph of the key-gates. Non mutable keys are connected by solid edges. If the new key-gate is inserted at the output (c) G10, it creates mutable edges (dotted lines) with the other key-gates and (d) G5, it creates non mutable edges (solid lines) with the other key-gates.

Insertion of key-gates

A protector can utilize the interference graph to embed key gates. An algorithm is utilized to embed key-gates. The algorithm has two stages: the introduction stage and the cycle stage. At first, the main key-gate is embedded at an irregular location in the circuit. At that point, the staying key-gates are inserted iteratively. In every emphasis, a blocking diagram of the key gates is built. For each gates in the net list, they decide, from the interference graph, the kind of edges regarding the previously inserted key-gates. A gate is chosen with the end goal that it includes just non-changeable edges to the diagram, and a key-gates is embedded at its yield. The diagram is then refreshed by including the new key-gates. On the off chance that none of the locations brings about a non-changeable edge with the current key gates, then the calculation embeds the following key-gates randomly. This methodology is rehashed for embedding all the key-gates.

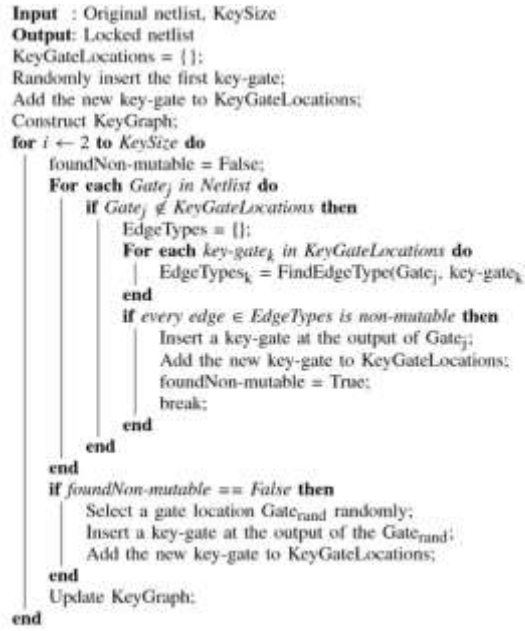

Fig. 6 Key gate insertion algorithm

Inference

In the proposed attack, it can recuperate the key-piece esteems for disconnected and mutable key-gates. The attack can't remove the keys for non-changeable key-gates. They had displayed the kinds of the key-gates embedded by various logic locking methods alongside the biggest coterie measure accomplished by each technique. The proposed strong logic locking algorithm offers expanded security against IP theft and figuring out attacks by embedding a bigger number of pair wise secure key-gates in a circuit.

Advantages

The flexibility of SLJI (Strong Logic Locking with Judicious Insertion of key gates) against the hill climbing attack is high. It counter measures the SAT-Based Attacks. The proposed system enhances the protection from the SAT-based attacks. It is conceivable to utilize ORF (One-way Random Function) to additionally reinforce the security of logic locking systems against existing SAT-based attacks.

Limitations

To better speak to impedance among key-gates and evaluate the viable key size for our logic locking algorithm, they likewise consider an elective metric, inner circle measure, already introduced by with regards to IC disguising. Clique size and Attacker's effort are significant confinements in SLJI.

Result and Discussion

To eradicate the IP piracy, the designers brainstormed many methods and successfully eliminated the counterfeiting of integrated circuits. In the fault analysis, the authors utilized key gates such that any wrong key causes a wrong yield to the attacker. Albeit, creating confusion to the attacker, it is vulnerable to path sensitization attack. To relieve way refinement attack, Yasin et al. [2] has proposed to embed the key-gates in chose areas to increase the interference between the key-gates. Though, the extraction of key gates might take longer than the process itself, it is still vulnerable to brute force attack. To overcome these issues, Rajit et al. [1] proposed a new logic encryption which involves an external key dependency block. It gives the surety from the fore mentioned attack including hill climbing attack.

References

[1] Rajit Karmakar, N Prasad, Santanu Chattopadhyay, Rohit Kapur and Indranil Sengupta, "A New Logic Encryption Strategy Ensuring Key Interdependency" IEEE 2017 30th International Conference on VLSI Design and 2017 16th International Conference on Embedded Systems

[2] M. Yasin, J. Rajendran, O. Sinanoglu, and R. Karri, "On improving the security of logic locking," IEEE Tran.on Computer-Aided Design of Integrated Circuits and Systems, no. 99, pp. 1–1, 2015.

[3] J. Rajendran, H. Zhang, C. Zhang, G. S. Rose, Y. Pino, O. Sinanoglu, and R. Karri, "Fault analysis-based logic encryption," IEEE Tran. On Computers, vol. 64, no. 2, pp. 410–424, 2015.

[4] J. A. Roy, F. Koushanfar, and I. L. Markov, "Epic: Ending piracy of integrated circuits," in DATE. ACM, 2008, pp. 1069–1074.

[5] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in Hardware Oriented Security and Trust (HOST). IEEE, 2015, pp. 137–143.

[6] Neil H.E. Weste and David Money Harris, 4th Edition "CMOS VLSI Design, A Circuits and System Perspective",2011, pp. 659-662.

Author Profile

Dr. M. Padmaa received B.E degree in Electronics and Communication Engineering from PSNA and M.E in VLSI Systems from REC, Trichy. Ph.D in Information Security from Anna university, Chennai. She is currently working as

Professor at Saranathan college of Engineering, Trichy. She has published 14 International journal papers and attended various national and international conferences.

S.Divyadarshini currently pursuing final year in Electronics and Communication Engineering at Saranathan College of Enginering, Trichy.

M.Keerthana currently pursuing final year in Electronics and Communication Engineering at Saranathan College of Enginering, Trichy.

T.S.Mohana Parameswari currently pursuing final year in Electronics and Communication Engineering at Saranathan College of Enginering, Trichy.

K.Mohana Priya currently pursuing final year in Electronics and Communication Engineering at Saranathan College of Enginering, Trichy.