This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

Threshold-defined Logic and Interconnect for Protection against Reverse Engineering

Jae-Won Jang[1]❖, Asmit De[2]❖, Deepak Vontela[3], Ithihasa Nirmala[4], Swaroop Ghosh[5] and Anirudh Iyengar[6]
Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA 24061, USA
Jjang3[1]@mail.vt.edu
School of Electrical Engineering and Computer Science, Pennsylvania State University, University Park, PA-16802, USA
{asmit[2], szg212[5], asi7[6]}@psu.edu; {deepakreddy[3], ithihasaredd[4]}@mail.usf.edu

***Abstract*—Securing the Intellectual Property (IP) from counterfeiting is an important goal towards trustworthy computing. Camouflaging of logic gates is a well-known technique to prevent an adversary from de-layering the chip and stealing IP. In this paper, we propose threshold voltage modulation to realize 2-input static camouflaged logic that can hide six functionalities. We extend the concept of threshold-voltage defined logic to propose multi-input camouflaged gates capable of hiding six 3-input Boolean functions (NAND, NOR, AOI, OAI, XOR, XNOR). We also propose interconnect camouflaging technique which hides the original connectivity of nets using a novel threshold-voltage defined pass transistor mux. Since threshold voltages are asserted during fabrication and are difficult to identify during optical Reverse Engineering (RE) based techniques, the adversary will be forced to launch a brute-force search. We present a thorough analysis of RE effort and overheads associated with the proposed camouflaging techniques. The proposed methodology is demonstrated using fabricated test-chip in 65nm technology.**

Keywords—Reverse Engineering; Threshold Voltage; Gate Camouflaging; Interconnect Camouflaging

I. INTRODUCTION

Reverse Engineering (RE) of an Intellectual Property (IP) [1-2] is a process of identifying its design, functionality, and structure. In the RE method, the adversary de-layers the IC, determines the gate functionalities and their connectivity information, and, reconstructs the netlist. This technique has been originally used by industries with the mindset of gathering information on its competitors, to confirm the functionality of their own design, and to ensure the legitimacy of circuits. However, the advanced adversaries can exploit this technique with an ill intention to steal and pirate the IP to illegally sell in the black market. RE is also a threat for defense sector due to sensitive IPs related to national security.

Camouflaging of gates have been proposed [3] to affordably hide the logic functionality and make the RE economically non-profitable or extremely difficult. The primary objective of gate camouflaging is to hide the functionality of a *few chosen gates* (since camouflaged gates are typically area, delay and power intensive) to increase RE effort of adversary while keeping power, performance and area overhead minimal. The camouflaged gates can assume functionalities such as AND, OR, XOR, etc. Although the exact gate functionality is hidden, the adversary can still create a partial netlist with other known gates and go through guess-and-validate process to reverse engineer the missing gate functionality. This is achieved by making a guess about the gate function, finding test patterns to confirm the guess, and then applying these patterns to both a partial netlist and a golden chip. If the outputs match, then the guess is correct; else the adversary guesses a new gate functionality and repeats the procedures. The RE effort is also shown which involves the time needed to identify all camouflaged gate functionalities.

It has previously been shown that careful camouflaging of ~10-40% gates can increase the RE effort significantly [4]. Table I shows a comparison of existing camouflaging techniques in terms of overhead, logic style and security vulnerabilities. Dummy contact [2], programmable standard cell [5], and filler cell [6] based camouflaging have been proposed in past for Integrated Circuits (IC). *The downside of these techniques is that they are either process costly or leave layout level clues*. For sequential circuits, additional logic (black) states are introduced in the finite state machine [7], which allow the design to reach a valid state only using the correct key. In combinational logic, XOR / XNOR gates are introduced to conceal the functionality [8-9]. Gate

TABLE I. COMPARATIVE ANALYSIS OF GATE CAMOUFLAGING TECHNIQUES

Feature / Technique	Hollow Via [2]	Programmable Standard Cell [5]	Filler Cells [6]	V_T Static Gates [10]	V_T Dynamic Gates [11]	MUX Gate [12]	CamoPerturb [24]
# of functions	3	Varies	Varies	6	2	$2^{2^{\wedge}m}$ for 2^m:1 MUX	Varies
Area overhead	3.06X	Not Disclosed	Not Disclosed	10.5X	4.25X	1.15X	1.09X
Delay overhead	1.32X	Not Disclosed	Not Disclosed	1.51X	11.48X	1.48X	1.01X
Power overhead	3.67X	Not Disclosed	Not Disclosed	8.75X	3.83X	N/A	1.19X
Static/dynamic	Static	Not Disclosed	Not Disclosed	Static	Dynamic	Static	Static
Security vulnerability / weaknesses	Requires hollow via tech.	Ctrl inputs have to be stored on-chip [14]	Filler cells do not drive any active logic [14]	Fab house will know transistor V_T	Fab house will know transistor V_T	De-synthesis attack [15]	Uses dummy contacts

Note: All comparisons are done with respect to a standard NAND gate.

❖ Both authors have equal contribution in this work.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

camouflaging based on the transistor threshold voltage (V_T) programmable switch that turns ON/OFF based on V_T assertion has been proposed in [10-11]. Other threshold voltage defined (TVD) gates based on dynamic logic have been explored in [29], along with improvements on it such as post-manufacture programming (PMP-TVD [30]) using HCI (Hot Carrier Injection), and pseudo-static TVD logic [31].

Split manufacturing [1] has been proposed to make the IC fabrication more secure and robust against RE. This technique separately manufactures the front-end (transistors) in an untrusted foundry whereas the back-end (interconnect) is manufactured in the trusted facility. This makes the RE and Trojan insertion more challenging for the adversary since the connectivity information is hidden in the untrusted foundry. Furthermore, since the front-end fabrication cost is higher than the back-end, the cost benefit of outsourcing the fabrication is still preserved. Although this technique is effective in preventing RE, it can be susceptible to yield loss during stacking due to via misalignment. Furthermore, it still requires trusted foundry and costly assembly process. Some recent advances in camouflaging techniques explore AND-tree structures [23] and min-term manipulation [24] to protect against de-camouflaging attacks such as Boolean satisfiability (SAT) [22]. Secure interconnect camouflaging have also been explored in literature that provides resilience to SAT-based attacks [27, 28]. MgO based dummy contacts for transformable interconnects have been explored in [33]. Obfuscating the interconnects by logic locking and split manufacturing have been explored in [34], while cross-bar architectures have been utilized to achieve logic locking in [35]. It should be noted that such dummy contact based logic locking requires process change and are expensive. Furthermore, [34] also relies on split manufacturing or a trusted BEOL (back end of line), which increases manufacturing cost and also results in yield loss. Other mux-based interconnect camouflaging requires some NVM storage to hold the secret select line information, which can lead to loss of security.

In this paper, we propose a V_T-defined multi-input camouflaged gates and a novel interconnect camouflaging technique to hide the connectivity information between gates. The proposed camouflaging techniques are achieved through V_T modulation (implemented by changing channel doping concentration during manufacturing) of transistors which leaves no layout trace. The proposed camouflaged gates can exhibit six Boolean functionalities. The proposed interconnect camouflaging technique relies on careful selection of nets based on the net selection methodology (Section V) to maximize the RE effort. The interconnect camouflaging technique is achieved by inserting multiplexers (muxes) in the design as illustrated in Fig. 1 using a C17 circuit as an example (from ISCAS85 benchmark [15]). The original connection is shown in thick black lines whereas the dummy connection is shown in light grey (highlighted in dashed-circle). If the adversary does not know the multiplexer

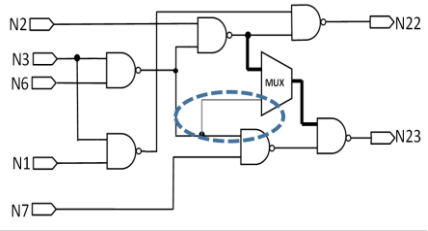


Fig. 1. Concept of interconnect camouflaging using mux. The real connection is shown using thick lines. The RE effort will involve guessing a connection and validating it by running test patterns.

select signal, he will resort to exhaustive reverse engineering. This, in turn, will increase the RE effort. The RE effort could be further increased by increasing the number of fake signals using N:1 mux. Since mux design is low-overhead in comparison to the camouflaged gates, the proposed interconnect camouflaging technique is light-weight while being effective. V_T-defined switch is used to design a multiplexer which is used to remove select signal requirement and to camouflage interconnects without incurring excessive overhead.

V_T modulation is a well-known technique that is used extensively in the semiconductor industry for trade-off between power, performance and robustness. Therefore, the proposed V_T based camouflaging comes without adding process cost. It is important to note that V_T could be reverse engineered by inspecting the transistor doping using Focused Ion Beam (FIB) and Scanning Electron Microscopy (SEM) [16]. However, this process is expected to be very expensive and since ICs contain billions of transistors, identifying the randomly placed camouflaged gates and successively identifying the dopant levels of the transistors in the camouflaged gates could be tedious, thereby making the reverse engineering process economically unviable. Therefore, the IP could still be protected from low-cost optical RE. Thus, since the V_T of a transistor is opaque to the adversary, it becomes difficult to guess the functionality of the circuit even if the adversary can optically inspect the layout of the camouflaged gate. As a result, the adversary resort to RE-intensive trial-and-error approach.

This paper extends our previous work on threshold-defined logic gates [17] [20]. We have included discussions on switch optimization, process variation considerations, V_{SN} and V_{SP} routing, and security implications in Section II. In addition, we have provided detailed analysis of 3- and 6-function camouflaged gates in Section III. Furthermore, we have proposed a novel interconnect camouflaging technique in Section V that utilizes a threshold voltage-defined pass transistor based mux to protect IPs. Sandia Controllability / Observability Analysis Program (SCOAP) [21] has been incorporated for all RE effort calculation and comparative results are presented throughout the paper. Various attack models for all of gate camouflaging techniques are presented in the Section VI to underscore the importance of camouflaging technique vulnerabilities. Validation of our

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

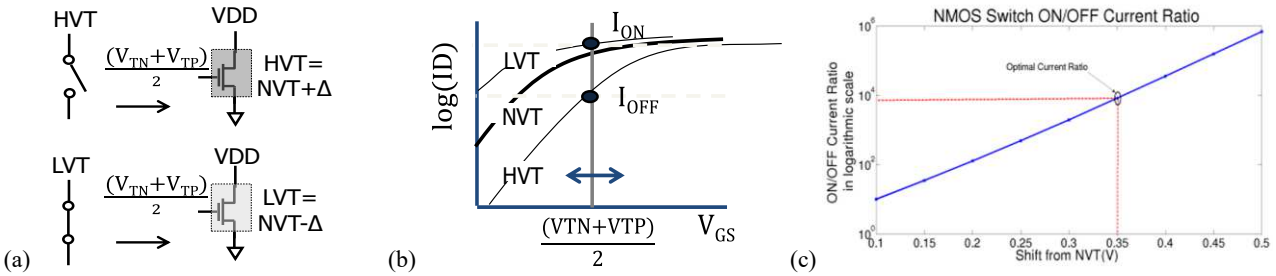


Fig. 2. (a) V_T programmable switch. HVT: OFF, LVT: ON. PMOS switch works similarly; (b) cartoon of I-V curves of NVT, HVT, and LVT transistors. The I_{ON} and I_{OFF} depends on the LVT and HVT values as well as on gate voltage biasing; and (c) LVT/HVT shift from NVT for high ON/OFF ratio (optimal current ratio).

technique using test-chip results is shown in Section VII Lastly, the overall comparative analysis of existing gate camouflaging techniques with respect to the proposed gate and interconnect camouflaging technique is presented in Table I.

In summary, we, (a) propose a 2-input camouflaged gate design capable of performing six complex Boolean functions; (b) propose a multi-input camouflaged gate design capable of performing six complex Boolean functions; (c) perform threat assessments on the proposed designs based on delay and power profile with respect to temperature; (d) propose an interconnect camouflaging technique using V_T-defined 2:1 and N:1 (where N = 4, 8 and 16) mux; (e) employ SCOAP based netlist generation algorithms for both gate and interconnect camouflaging and analyze the respective area, power and delay overheads; (f) quantify RE effort for the proposed camouflaging techniques using basic SAT-based solvers [22]; and (g) experimentally evaluate our proposed technique on a 65nm test-chip.

II. Design and Analysis of V_T-Defined Switch

In this section, we present the switch design and optimization and discuss design and security concerns.

A. Switch Design

We propose a switch that turns ON/OFF based on V_T asserted on it. The switch is realized by using conventional NMOS transistors with the gate biased at the mid-point between nominal NMOS and PMOS threshold voltages i.e., $0.5(V_{TN}+V_{TP})$ (Fig. 2(a)). Therefore, the switch conducts when low V_T (LVT) is assigned during manufacturing. This is since $V_{GS} = 0.5(V_{TN}+V_{TP}) >$ LVT. The switch stops conducting when high V_T (HVT) is assigned ($V_{GS} <$ HVT).

The cartoon of transistor I-V curves for NVT, LVT and HVT transistor is shown in Fig. 2(b). The I_{ON} and I_{OFF} that can be obtained by assigning LVT and HVT is also shown. A good V_T-defined switch should offer high I_{ON} and low I_{OFF}. Fig. 2(c) depicts the I_{ON}/I_{OFF} ratio with respect to the offset in LVT/HVT values compared to NVT. It can be observed that the gate voltage, HVT, LVT values and transistor sizes can be tuned to maximize the I_{ON}/I_{OFF} ratio. For NMOS-switch, higher HVT values and lower gate voltage is good for I_{OFF} (leakage) whereas lower LVT and higher gate voltage is good for I_{ON} (performance).

B. Switch Optimization

It is noteworthy that LVT and HVT in a process technology is optimized based on factors such as, leakage and performance of combinational logic. Therefore, it is likely that the proposed camouflaging will end up using the pre-defined HVT and LVT values. However, if the optimization option is made available to the camouflaging designer, then security could be factored in along with leakage and performance to decide the optimal values of HVT and LVT as described in this Section.

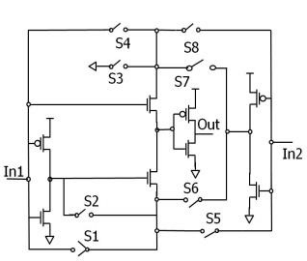
C. Process Variation Considerations

One valid concern with the proposed threshold-defined switch is the impact of process variation. However, it should be noted that the threshold-voltage variation is a function of transistor geometry. Therefore, the width of threshold-defined switch is kept larger to minimize the effect of variation and keep the LVT and HVT values distinct from NVT values. Furthermore, when standard LVT and HVT values are used without optimization, a fixed V_{SP} and V_{SN} may not be enough to cover the process corners. In such a scenario, the V_{SP} and V_{SN} values can be dynamically tuned based on the process corner using PVT measurement circuits on chip. However, this will increase circuit complexity and add to the area overhead.

D. Routing of V_{SN} and V_{SP} and Security Implications

The proposed camouflaging technique requires routing of gate voltages V_{SN} (for NMOS) and V_{SP} (for PMOS) signals to the gates of the threshold-defined switches. Therefore, the adversary will be able to know the position of the switches after RE. In fact, the adversary will be able to identify the location of the camouflaged gates during the RE. Therefore, V_{SN} and V_{SP} signals don't provide any extra information to the adversary. Note that it is not possible for the adversary to know the voltage levels of these two DC signals during RE. Furthermore, the voltage levels don't reveal any information regarding the state of the switches which is governed by the V_T assignment. Since V_{SP} and V_{SN} signals drives the transistor gates, they don't carry significant currents. Therefore, the drop in these signals is minimal and they can be routed with less restrictive constrains to minimize overhead. Since the number of camouflaged gates in the design is 5%-15% the routing complexity is expected to be low.

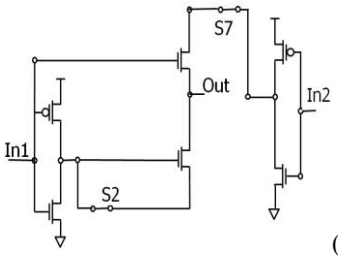
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems



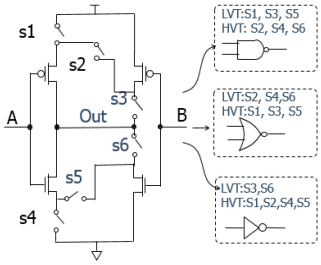
(a)

Logic	LVT Switches
AND	S2, S7
OR	S3, S6
NAND	S1, S8
NOR	S4, S5
XOR	S6, S8
XNOR	S5, S7

(b)



(c)



(d)

Fig. 3. (a) Proposed 2-input 6-function camouflaged gate; (b) selection of switches required to exhibit respective functionality (remaining switches are programmed HVT); (c) example portraying AND logic selection; and (d) proposed low-overhead 2-input 3-function camouflaged gate.

III. Design and Analysis of 2-Input Camouflaged Gates

In this section, we will discuss the design and analysis of proposed two-input camouflaged gates that exhibit 6 functions and 3 functions (lower overhead) [17].

A. Proposed Camouflaged Gate (2-input 6-function)

Fig. 3(a) depicts the schematic of the proposed two-input camouflaged gate. The camouflaged gate hides six logic functionalities (AND, OR, NAND, NOR, XOR, and XNOR). A function is selected by asserting LVT to the corresponding switches listed in Fig. 3(b). For example, by setting S2 and S7 to LVT and every other switch to HVT, AND logic can be realized as shown in Fig. 3(c).

B. Low-Overhead Camouflaged Gate (2-input 3-function)

The camouflaged gate proposed above offers high resistance to RE since it exhibits 6 functionalities. However, it comes at the expense of design overhead. We propose a low-overhead flavor of camouflaged gate with 3 functions i.e., NOT, NAND and NOR (Fig. 3(d)). This design is based on static CMOS. The switches that have to be asserted with HVT and LVT are also seen in the figure.

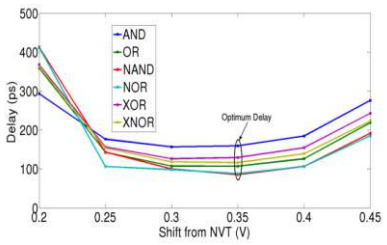
C. Design Space Exploration

For the design space exploration of these proposed gates, we have used PTM 45nm technology [18]. The LVT and HVT values are chosen by determining their offset (Δ in Fig. 2(a)) from NVT value. For example, if the NVT of NMOS transistor is 0.62V, an offset of 0.1V (i.e., Δ = 0.1V) means that the LVT is 0.52V and HVT is 0.72V. Additionally, we evaluate the delay of various gate topologies to explore the optimal offset voltage. The gate delay with the offset of LVT/HVT values from NVT is shown in Fig. 4(a). The higher offset shows lower delay. This is because lower LVT reduces the resistance of ON switch whereas higher HVT increases resistance of OFF switch. In addition, the impact of switch bias voltage on delay is shown in Fig. 4(b). A higher gate voltage lowers the resistance of ON switch making the circuit faster. Considering the optimal delay from Fig. 2(c) and 4(a)-(c), an offset voltage of 0.35V from NVT is selected for LVT/HVT. The switch bias voltage is selected to be 0.68V. Note that the analysis is done for the NMOS switch. Moreover, similar analysis holds true for PMOS switch.

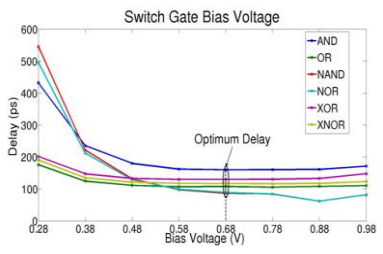
In addition, we optimize this design to lower delay overhead by: (i) separating the P and N switch gate voltages and biasing them to improve the robustness; and (ii) sizing the transistors accordingly. Note that the performance and area of the proposed camouflaged gates are strongly correlated to the resistance of ON and OFF switches in the path. Considering the widths of all the switches, area of the proposed camouflaged design is calculated to be 2.64μm^2 and 1.44μm^2 for 6-function and 3-function camouflaged gate respectively.

D. Analysis of Camouflaged Gates

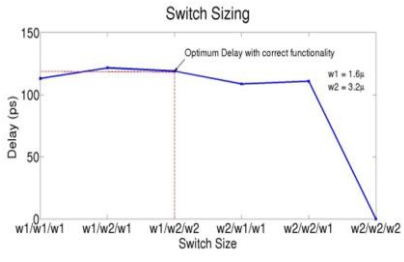
Table II shows the comparative analysis of the 6-function camouflaged gate and Table III shows the comparative analysis of the 3-function low-overhead camouflaged gates with some recent works on threshold voltage defined gates, such as TVD [29] and PMP-TVD[30]. Although, our area overheads are slightly higher than [29], our design outperforms both [29] and [30] in terms of delay overhead, while keeping the power overhead comparable to the others. Although the TVD gates can implement 16 Boolean functionalities, they are implemented in dynamic logic. Hence



(a)



(b)



(c)

Fig. 4. Selection of V_{SN} and offset from NVT: (a) delay optimization for various gate topologies; (b) switch gate voltage biasing for delay optimization; and, (c) switch sizing for optimimum delay with correct functionality.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

TABLE II. OVERHEAD COMPARISON OF 6-FUNCTION CAM GATE WITH RESPECT TO STANDARD CELLS

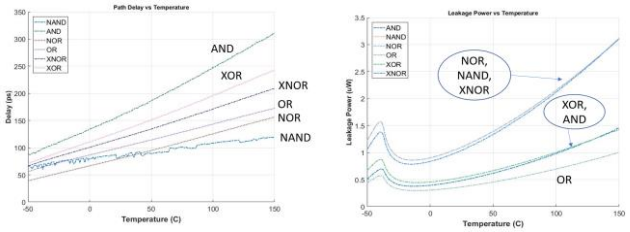
Functionality	Area	Delay	Power
AND	11.8X	1.6X	17.4X
OR	11.8X	1.4X	14X
NAND	11.9X	2.9X	23X
NOR	11.9X	2.7X	21.8X
XOR	5.9X	1.5X	10.6X
XNOR	5.9X	1.7X	1.8X

TABLE III. COMPARISON OF PROPOSED 3-FUNCTION CAM GATE WITH SIMILAR WORKS WITH RESPECT TO STANDARD CELLS

	3-Func. CAM			TVD[29]			PMP-TVD[30]		
	Area	Delay	Power	Area	Delay	Power	Area	Delay	Power
NAND	6.89X	1.98X	4.53X	3.7X	3.2X	1.6X	7.3X	6.6X	9.2X
NOR	6.89X	1.51X	5.14X	3.7X	2.6X	1.9X	7.3X	5.4X	4.0X

they are best suited for low complexity circuits with limited area budgets, but not as scalable as the proposed static logic implementations. It can be observed that our 3-function camouflaged gate displays lower overhead with respect to standard gates than 6-function camouflaged gates. This is largely due to low-overhead design requiring fewer NVT transistors (3 INVs in 6-function while only 2 INVs required for 3-function). The proposed gate should be used judiciously in the design to minimize the overall design overhead. System level techniques such as converting off-critical path gates (lower delay overhead), low-activity gates (lower power overhead) and more complex gates (lower area overhead) to camouflaged gate can be used to minimize the overheads.

For thermal analysis, we swept the temperature from -25C to 150C, to account for unspecified operating temperatures (assuming specified operating temperature to be between -10C and 90C) that can be exploited by adversary *to create side channel (later discussed).* Fig. 5(a) shows the plot for the gate delays with temperature variations for each of the six configurations. The leakage power consumption with temperature variations is shown in Fig. 5(b). The gate delay increases with temperature. This is primarily due to the reduction of V_T at higher temperature turning the HVT switches weakly ON and contending with the signal. Since the



(a) (b)

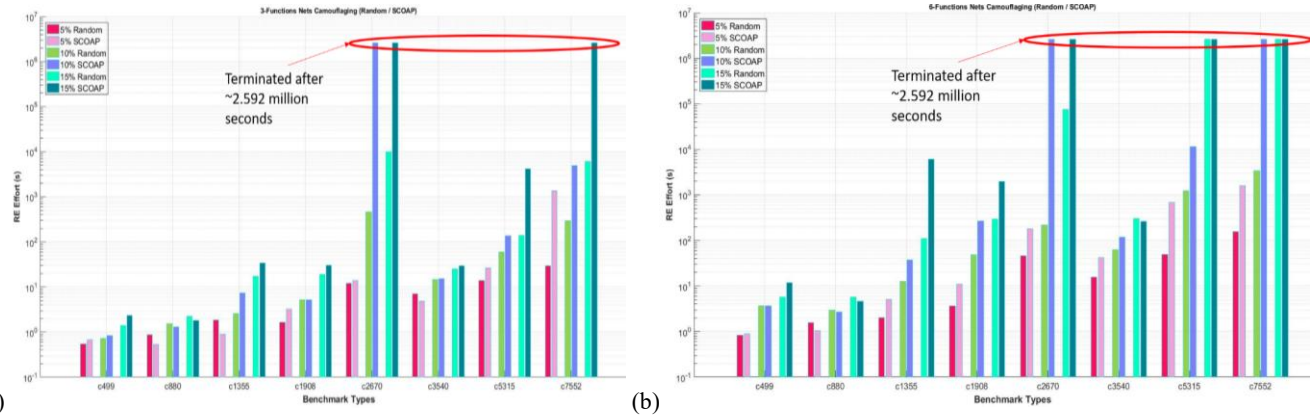
Fig. 5. (a) Delay; and, (b) power profile with temperature variations of the 2-input camouflaged gate configurations.

camouflaged gate delay depends on the selected functionality one can conclude that a single camouflaged gate can leak gate information through delay and leakage signatures. However, our detailed analysis of multiple camouflaged gates in circuit indicate that the side channel information is naturally obfuscated (Section VI).

E. Simulation Results

We tested our camouflaged circuit with basic SAT-based solver proposed in [22]. We replaced gates using a SCOAP based algorithm and the random replacement strategy which selects gates randomly. The SAT-based solver source code is publicly available to be used in the main author's webpage [22]. This simulation was executed on an Intel Core i7-6700 3.4GHz Quad Core processor with 16Gb of RAM running Ubuntu 16.04 LTS x86_64 Operating System.

Fig. 6 shows the simulation results of RE effort for gate camouflaging using (a) 3-function and (b) 6-function. The RE effort is written in terms of seconds (System CPU time) and the results that are hovering above ~10^6 seconds were deemed to be unsolvable (highlighted with red circle on the figures) and had to be manually terminated. Among obtained simulation results, the longest time the SAT-based solver took without having to manually terminate was 74456 seconds for c2670 benchmark using 6-function using 15% random camouflaging technique. These RE effort results are comparable to some recent camouflaging techniques [23, 24]. Analytical proof of SAT-resilience of our technique is out of scope for this paper, however, such proofs have already been demonstrated in [27, 28]. Since our camouflaging technique



(a) (b)

Fig. 6. RE effort using SAT-based solver for 2-input: (a) 3-function; and (b) 6-function gate camouflaging (random / SCOAP)

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

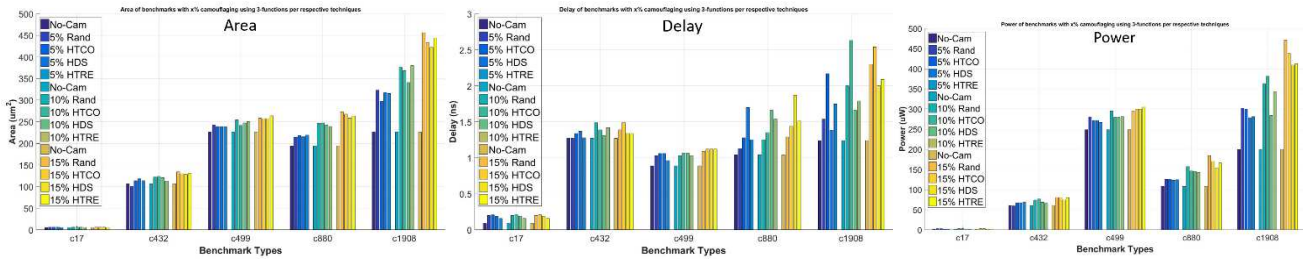


Fig. 7. Area, delay and power of benchmarks with x% (x=5, 10, 15) camouflaging with listed techniques (Random, HTCO, HDS, and HTRE) using 3-functions camouflaged gate.

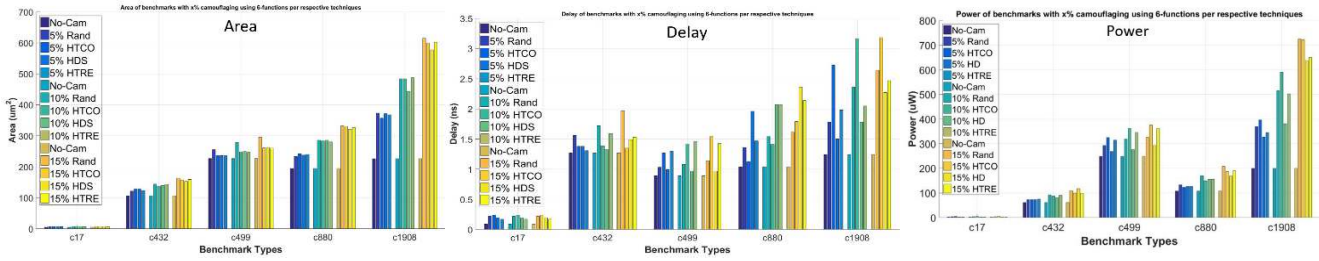


Fig. 8. Area, delay and power of benchmarks with x% (x=5, 10, 15) camouflaging with listed techniques (Random, HTCO, HDS, and HTRE) using 6-functions camouflaged gate.

is based on a MUX-based approach, it is expected to provide similar SAT-resilience guarantees.

We can observe that by increasing the number of functions and using our proposed camouflaging strategy, the RE effort improved and few circuits became unsolvable although they were solvable for 3-function. Additionally, it can be noted that there are few exception benchmarks which become unsolvable independent of its benchmark size (such as c2670 breaking the norm of linear increase of the RE effort with respect to gate counts of benchmarks). Larger benchmark circuits can also be simulated to evaluate the effectiveness in imposing higher RE effort. However, such large benchmark simulation is beyond the scope of this paper. Our results are based on a basic SAT-solver, hence, smaller benchmark circuits may not be as resilient under more sophisticated SAT-solver based attacks.

The overheads associated with 5%, 10% and 15% camouflaging are shown in Fig. 7-8. We compared the overheads for the different percentages of camouflaging based on random, SCOAP/HTCO (explained in the following section), HDS and HTRE replacement mechanisms (the details of the last two can be found in [36]).

F. Camouflaging Strategy and Evaluations

Since camouflaged gates are area, delay and power intensive, they cannot be used frequently in the design. Gate selection techniques such as, random, non-resolvable and output corruptibility have been proposed [2] and can be used in this work. However, we employ a controllability (CC) and observability (Obs) based algorithm (HTCO) to identify interconnects/gates based on quantifiable values to maximize RE effort. Controllability and observability metrics have been widely used in literature to analyze testability of digital circuits [25, 26]. The difficulty of controlling and observing logical values of internal nodes from circuit I/O determines the ease of testability of the circuit. Hence it follows that these metrics are suitable for determining camouflaging complexity, as the primary objective of camouflaging is to increase the RE effort for determining circuit functionality. We first compute the CC and Obs values using SCOAP [21] for every net and its number of fan-outs in a circuit. The '0' and '1' controllability (CC0 and CC1) and observability values provides a relative difficulty of controlling and observing a logic signal of a particular net. By selecting the net with low CC0, CC1 and Obs values, it is possible to increase the RE effort of adversaries. Note that the controllability and observability of the net is assigned the same value as the controllability and observability of the gate that is driving the net. For the nets with fan-outs (FO), the controllability and observability is propagated to all fan-out nets.

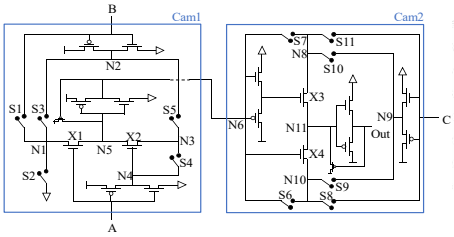
Algorithm 1 Gate Camouflaging Algorithm

1: **procedure** GATE CAMOUFLAGING($Input1$)
2: $Input1 = Synthesized\_ISCAS85\_netlist$
3: $Input2 = Gate\_Replacement\_Percentage$
4: $Input3 = benchmark\_SCOAP\_sorted$
5: $Output = finalNetlist$
6: **while** $Input1 ==$ true **do**
7: $Step1 \rightarrow G = CreateGraph(Input1)$
8: $Step2 \rightarrow TraverseGraph(G) \rightarrow RecordValues(CC\&Obs)$
9: $Step3 \rightarrow metric = CC0 + CC1 + Obs$
10: $Step4 \rightarrow newGraph = DescendingSort(metric)$
11: $Step5 \rightarrow Input2 = PrioritizeSelect(newGraph)$
12: $Step6 \rightarrow finalNetlist = GateInsertion(Input2, Input3)$
13: **end while**
14: Return $finalNetlist$
15: **end procedure**

Fig. 9. Netlist generation algorithm for gate camouflaging

Fig. 9 displays the netlist generation algorithm for the gate camouflaging technique using the controllability and observability metrics (SCOAP) which is implemented in C++ and tested using HSPICE simulation. The algorithm imports Verilog benchmarks and finds controllability / observability values of the gates (step 2) and then assigns these values to the output nets (step 3). Upon obtaining these parameters, we sort the output nets in descending order based on

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems



Logic	LVT Switches
NAND	S3,S4,S7,S8
NOR	S2,S5,S6,S11
AOI	S3,S4,S6,S11
OAI	S2,S5,S7,S8
XOR	S1,S5,S8,S10
XNOR	S1,S5,S9,S11

(a) (b)

Fig. 10. (a) Proposed 3-input 6-function camouflaged gate showing Cam1 and Cam2 blocks, (b) selection of switches required to exhibit respective functionality (remaining switches are programmed HVT).

CC0+CC1+Obs value (step 4). When nets are sorted, we select dummy / fake nets based on the priority of CC0, CC1, Obs, and fan-outs parameters (step 5). By selecting the fake nets that are difficult to control and observe, we can further improve RE effort (This is further evident from observing the output shown in Fig. 6). Afterwards, camouflaged gates are inserted, and the new netlist is created. This netlist is used for the Synopsys Design Compiler [19] to perform synthesis and to evaluate the overall design in terms of area overhead, propagation delay, and power consumption compared with the original ISCAS85 benchmarks (shown in Fig. 7-8).

IV. Design and Analysis of 3-input Camouflaged Gates

In this section, we will extend the 2-input camouflaged gates further and propose three-input camouflaged gate that exhibits 6-function [20].

A. *Proposed Camouflaged Gate (3-input 6-function)*

The proposed 3-input camouflaged gate is shown in Fig. 10(a). This design consists of 6 inverters, 4 pass transistors, 2 level restorers and 11 V_T-defined switches. It is a two-stage design with the first stage generating a Boolean output based on the first two inputs, A and B. The third input C is attached to the second stage. The first stage essentially performs 2-input AND, OR and XOR functions. The second stage can perform 2-input NAND, NOR, XOR and XNOR functions. Combining these two stages in series generates the different 3-input Boolean functions. The V_T-defined switches, numbered from S1 to S11 can be selectively set to HVT or LVT to configure the gate to dynamically modify the circuit to behave as a particular function. Fig. 10(b) shows the six different functions that the camouflaged gate can perform along with the corresponding switches that needs to be turned ON to configure the circuit. The switches are in an OFF (ON) state when it is set to HVT (LVT).

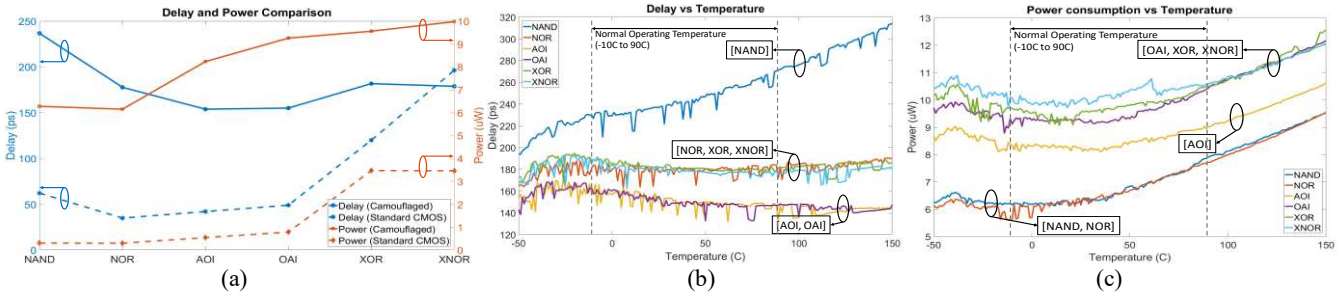
The six functions performed by the proposed gate are NAND, NOR, AOI, OAI, XOR and XNOR. All the switches are initially set to HVT. In case of the NAND gate for example, in the first stage, switches S3 and S4 are set to LVT to turn them ON. The inputs to the first stage are the first two inputs A and B. This makes the first block function as an AND gate performing AB. In the second stage, switched S7 and S8 are set to LVT to turn them ON. The inputs to the second stage are the third input C and the output of the first stage, designated as node N6. This makes the second block function as a two input NAND gate using the aforementioned two inputs. Thus, the final output from the second stage is (ABC)', i.e., NAND on inputs A, B and C. The other five functions are generated in a similar manner using the switches in Fig. 10(b).

The logic blocks are designed based on a 2-input pass transistor logic. The inputs are used in normal and complemented form by using CMOS inverters. The outputs in each stage are obtained in complemented form by using additional inverters and level restorers as the output at nodes N5 and N11 do not generate the full swing from 0 to 1. The four pass transistors (X1, X2, X3 and X4) are NMOS transistors set to normal V_T.

B. *Simulation Results*

Similar design space exploration from 2-input camouflaged gates is applied to both 3-input and N-input camouflaged gates. We used PTM 45nm technology [18] for the design and analysis. However, the inverters are sized with a β-ratio of 2.25, where the NMOS width is chosen as 1.6µm. The NMOS pass transistor widths are set to 3µm. The width of the V_T-defined switches is set to 3.2µm. Due to the incomplete swings at the outputs of Cam1 and Cam2 blocks, PMOS level restorers are used to generate a complete swing. The level restorers for Cam1 and Cam2 blocks are sized at 0.2µm and 0.4µm respectively. The simulations are performed assuming an operating temperature of 25C.

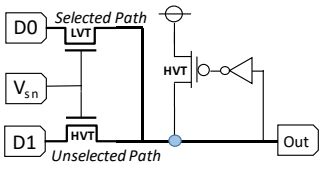
Fig. 11(a) shows the calculated delay and power for the six functions of the 3-input camouflaged gate compared to standard 3-input CMOS implementations. The average delay



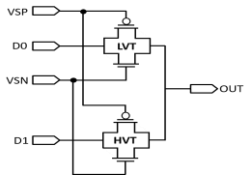
(a) (b) (c)

Fig. 11. (a) Delay and leakage comparisons for the 6 camouflaged configurations; temperature analysis on (b) delay profile and (c) power profile of the 3-input camouflaged gate configurations.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems



(a)



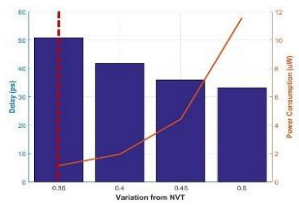
(b)

(c)

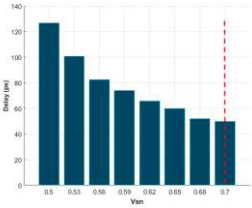
Type	Delay (ps)	Power (uW)	Area (um²)
2:1 NMOS MUX	25.2	0.57	0.598
4:1 NMOS MUX	39.4	0.81	1.098
8:1 NMOS MUX	50.8	1.16	2.1
16:1 NMOS MUX	73.1	1.88	4.1
2:1 NAND Gate	40.4	0.205	0.208

Type	Delay (ps)	Power (uW)	Area (um²)
2:1 TR MUX	43.6	8.1	1.31
4:1 TR MUX	62.46	12.2	2.2
8:1 TR MUX	98.3	28.6	4.27
16:1 TR MUX	147.9	44	8.41
2:1 NAND Gate	40.4	0.205	0.208

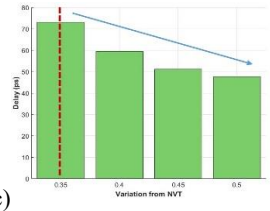
Fig. 12. (a) The proposed pass transistor NMOS-only based 2:1 mux; (b) the Transmission (TR) gate based 2:1 mux; and (c) attributes of the proposed N:1 mux for NMOS-only mux and TR-gate mux.



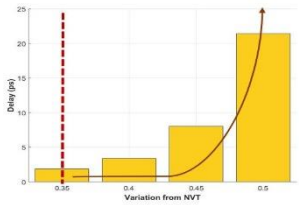
(a)



(b)



(c)



(d)

Fig. 13. Selection of V_{SN} and offset from NVT: (a) 8:1 mux delay and leakage vs offset; (b) 8:1 mux delay vs V_{SN}; (c) 16:1 mux delay vs offset; and, (d) 16:1 mux leakage vs offset. The optimal choice of offset is also shown by dashed lines.

is 178ps (3.03X overhead compared to standard CMOS) and average dynamic power is 8.282 µW (12.33X overhead compared to standard CMOS) for the 6 configurations. The total transistor count for the 3-input camouflaged gate is 29, compared to the standard 3-input CMOS implementations having transistor counts of 6 for NAND, NOR, OAI, AOI (5X overhead), and 30 for XOR and XNOR (no overhead). Since the proposed gate fuses 6 functionalities, the area benefit with respect to cumulative sum of 6 discreet normal gates is approximately 65%.

We repeat the thermal analysis on 3-input camouflaged gates. Fig. 11(b) shows the plot for the gate delays with temperature variations for each of the six configurations. The power consumption with temperature variations is shown in Fig. 11(c). From the graphs it can be seen than the NAND configuration delay gradually increases with temperature. At higher temperatures, the gate experiences glitches due to higher delays. The remaining five configurations have consistent delays, reaching the highest at approximately -25C. The average delay at high operating temperature (100C) is similar to that at normal temperature (25C). Beyond 100C, the curves tend to rise again. The initial consistency of the delay could be a result of the increasing I_{ON} due to the reduction in V_T. At much higher temperatures, the delay increases due to the reduction in carrier mobility. The power profiles are nearly identical for all the six functions, first reaching a peak around -40C, then stabilizing around 20C, and finally increasing steadily above 50C. The average power consumption at 100C is 1.18X higher than at 25C.

V. Interconnect Camouflaging Technique

In this section, we introduce a novel V_T-defined mux used for interconnect camouflaging, design space exploration and methodology to identify interconnects that can be obfuscated.

A. Proposed Multiplexer Design and Challenges

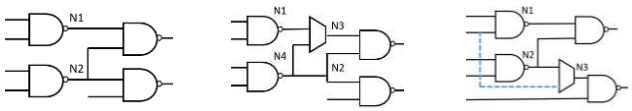
The V_T-defined switch [10] is optimized to suit the mux application. In the proposed mux, the real path contains LVT pass transistor and the fake paths contain HVT pass transistor (Fig. 12(a)). This eliminates the need of a mux select input as V_T value inherently determines the input selection. Since an NMOS transistor cannot pass a strong input '1', we incorporate a level restoring weak HVT PMOS transistor (highlighted with dashed-circle in Fig. 12(a)) to pull the NMOS pass transistor output to full-rail. The level restoring transistor helps full voltage swing of the degraded input and improves the low-to-high transition.

Furthermore, it eliminates the static current from the output inverter. The sizing of this level restoring PMOS transistor is done carefully so that it does not contend with the mux inputs. The alternative design technique to avoid level restoring transistor is to use full transmission gates (with NMOS and PMOS in parallel as shown in Fig. 12(b)). This method will allow both strong input '0' and '1' to be passed through the muxes, but incurs significant power, delay, and size overhead due to requirement of large PMOS transistors. From Fig. 12(c), it can be seen that transmission gate design increases area and power overhead especially for wide input mux designs. The pass transistor NMOS-only mux logic allows the proposed design to be compact without incurring significant overhead. The 2:1 NMOS mux is comparable to 2-input minimum sized NAND gate in terms of delay.

B. Design Space Exploration

For the design space exploration, we also used PTM 45nm technology [18]. The LVT and HVT values are chosen by determining their offset (Δ in Fig. 2(a)) from NVT value. We sweep both offset (Δ) and gate voltages (V_{SN}) and calculate the delay and leakage power of 8:1 and 16:1 mux circuit. The offset voltage (Δ) is swept from 0.35V to 0.5V in steps of 0.05V for NMOS. The switch gate voltage (V_{SN}) is swept from 0.1V to 0.5V in steps of 0.05V. Fig. 13(a) shows the delay and leakage power values with offset (Δ) and Fig. 13(b) shows the delay when gate voltage (V_{SN}) are varied. Using the information from these two plots, we choose the optimum values of Δ (= 0.35V) as we prioritize minimizing the leakage value due to pass transistor design. We have selected V_{SN} value to be 0.7V to balance out the increased delay resulted

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems



(a) (b) (c)

Fig. 14. Example of qualified nets selection: (a) original circuit; (b) single-fan-out net which is selected for mux insertion. Since N1 cannot float, the adversary can easily guess that N1 connects to N3. We disqualify such nets for mux insertion; and (c) multi-fan-out net N2 is selected for mux insertion. Adversary cannot guess connection between N2 and N3. Such nets are qualified for selection.

Algorithm 2 Interconnect Camouflaging Algorithm

```
1: procedure INTERCONNECT CAMOUFLAGING(Input1)
2:     Input1 = Synthesized_ISCAS85_netlist
3:     Input2 = Net_Replacement_Percentage
4:     Input3 = benchmark_SCOAP_sorted
5:     Output = finalNetlist
6:     while Input1 == true do
7:         Step1 → G = CreateGraph(Input1)
8:         Step2 → TraverseGraph(G) → RecordValues(CC&Obs)
9:         Step3 → metric = CC0 + CC1 + Obs + FO
10:        Step4 → newMetric = assignFanOutNets(metric)
11:        Step5 → newGraph = DescendingSort(newMetric)
12:        Step6 → Input2 = PrioritizeSelect(newGraph)
13:        Step7 → finalNetlist = MuxInsertion(Input2, Input3)
14:    end while
15:    Return finalNetlist
16: end procedure
```

Fig. 15. Netlist generation algorithm for interconnect camouflaging

from selecting the lowest Δ value. These attributes are used for simulating 2:1, 4:1, 8:1, and 16:1 muxes. A similar trade-off study is conducted between the delay and leakage power for 16:1 mux (Fig. 13(c)-(d)).

C. Selection of Qualified Nets

To maximize the RE effort, it is critical to camouflage the nets that cannot be reverse engineered through simple intuition. For example, if net N1 (which is a single fan-out net) in Fig. 14(a) is camouflaged using a mux as shown in Fig. 14(b), then reverse engineering becomes straightforward. This is true since N1 cannot float in a valid design. This leaves the adversary to conclude that N1 and N2 are connected without running any simulation. We discard such single fan-out nets from the selection algorithm. In contrary, if a multi-fan-outs net such as N2 is selected for mux insertion, then the adversary cannot figure out the connection between N2 and N3 (Fig. 14(c)). Such nets are considered qualified nets in the proposed camouflaging procedure.

D. Net Selection Methodology

To select interconnects for camouflaging, we employed a similar methodology used to select gates which was explained in the Section III(E). However, for interconnect selection strategy, we additionally incorporate the fan-out (FO) values on top of CC and Obs values. Incorporating the number of fan-outs increase a circuit's RE effort, as previously explained (Fig. 14). Therefore, following modifications are made on the gate camouflaging algorithm (Fig. 15):

1) When we assign the metric parameter in step 3, we now include fan-out values of respective gates for metric calculation.
2) We add an additional step (step 4) which calculates the number of fan-outs of the nets and assign them to the corresponding parent net. This new metric value will be used for sorting.
3) Mux insertion rather than gate insertion in step 7.

In addition to the above technique, we also select nets randomly for camouflaging. The fake nets are randomly selected and the RE effort and overheads are compared with respect to the CC/Obs based selection methodology.

TABLE IV. AVERAGE OVERHEAD PERCENTAGE OF N:1 MUX FOR 5% CAMOUFLAGING NETS

Gate	Area	Delay	Power
2:1 mux	15%	20%	14%
4:1 mux	22.43%	38.12%	13.99%
8:1 mux	25.32%	41.08%	16.23%
16:1 mux	34.99%	49.29%	19.41%

E. Simulation Results and Analysis

In this section, we evaluate the design overhead using Synopsis Design Compiler [19] for ISCAS85 benchmarks [15]. Since V_T-defined muxes are not included in standard cell library, we have created a liberty file of the proposed muxes with values characterized using HSPICE simulation. We evaluated area, delay, and power of benchmarks replaced with 2:1 to 16:1 muxes for 5% camouflaging using the CC/Obs based net selection methodology. Compared to the original ("No Mux") design, the average overhead is found to be 15% (area), 20% (delay) and 14% (power) for 5% camouflaging (Table IV). The values for 10% camouflaging are 26%, 41% and 22%. For 15% camouflaging, the values are 33%, 44% and 29%. From these results, we can observe the linear relation of overhead with respect to the number of camouflaged nets. Explanation of these results are: 1) the area overhead linearly increases as wider muxes require additional transistors; 2) the delay overhead increases due to the longer propagation delay from cascaded mux design; and 3) wider muxes incur additional power. Our results are comparable to the interconnect obfuscation technique in [34], providing linear overheads. Although our performance overheads are slightly higher than [34], it is to be noted that [34] considered *m=2* (2 wires per input) for their evaluated design, while our technique can uses up to 16:1 mux, thereby providing more complexity in the number of configurations.

The interconnect camouflaging technique using 8:1 mux was tested using the SAT-based solver [22]. For this comparison, we have omitted the random camouflaging technique depicting SCOAP to provide much improved result. Therefore, we have only compared SCOAP methodology of interconnect camouflaging using 8:1 mux with respect to 3-function and 6-function gate camouflaging technique. This result is depicted in Fig. 16, where it can be seen that 8:1 mux interconnect camouflaging technique yielded in average improved RE efforts of 117%, 74%, and 106% for 5%, 10%, and 15% camouflaging respectively with respect to 6-function camouflaged gates. It is important to note that although the 8:1 mux interconnect camouflaging technique resulted in improved RE effort, it incurred much higher overhead.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

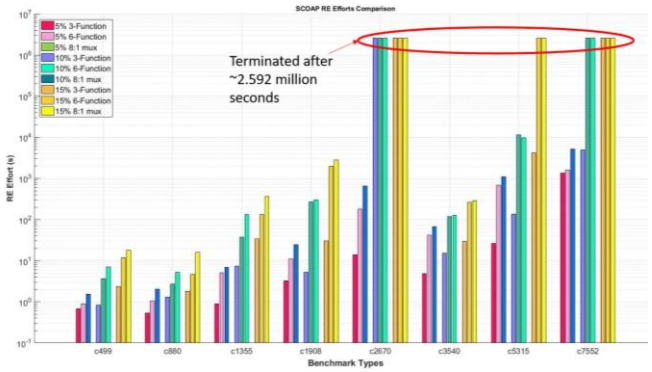


Fig. 16. RE effort comparisons for 3-function gate camouflaging, 6-function gate camouflaging, and 8:1 mux interconnect camouflaging.

Therefore, the interconnect technique needs to be sparingly used and on the occurrence where the robustness is prioritized over the possible overhead concerns. The delay in the combinational logic can somewhat be alleviated by reducing the clock frequency or by using LVT transistors for the gates in the critical path to optimize the delay for that path. If further logic optimizations are required, it may need retiming, in which case further logic validation needs to be performed.

VI. Attack Models

In this section, we explore the possible attack models on the proposed 2-input and 3-input camouflaged gates.

A. Leakage Side Channel

Leakage power signature of a circuit can serve as another important side channel that can be exploited by the adversary to identify the functionality of a camouflaged gate. Fig. 17(a) and Fig. 18(a) show the leakage power variations of a single 2-input and 3-input camouflaged gate respectively with temperature when the inputs are set to 2'b00 and 3'b000. The leakage profile shows a steady increase in power with increase in temperature. For a single 2-input camouflaged gate there are distinct cluster of NAND+XOR+OR and NOR+AND+XNOR especially at high temperature. The adversary can exploit it to identify the gate functionality. For 3-input camouflaged gates, there are two distinct clusters, with one containing the profile for NAND only, and the other containing the rest. This shows that the adversary can identify NAND by its lowest leakage (our study refutes this though).

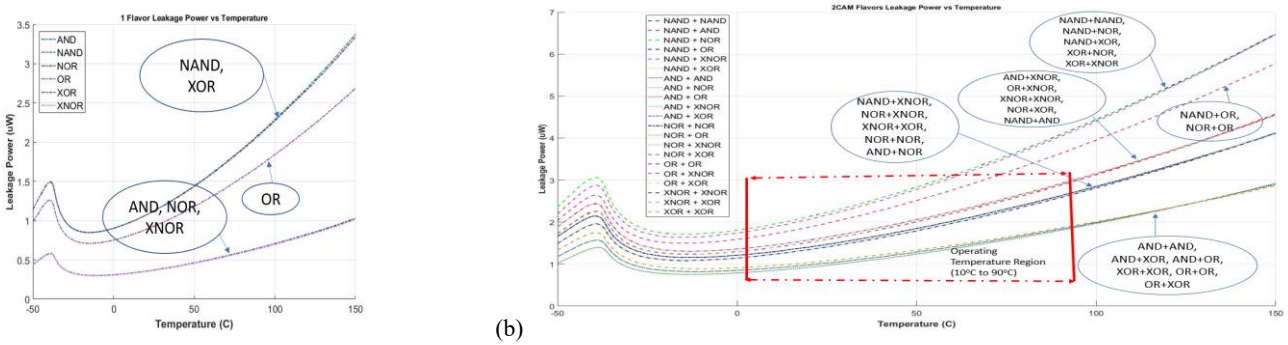
Fig. 17(b) shows the leakage due to two 2-input camouflaged gates and Fig 18(b) shows the leakage for combinations of two 3-input camouflaged gates. For the combinations of two 2-input gates, there are six different clusters at high temperature (~90C). However, the gate combination with XNOR (e.g., XNOR+NOR) is in specifically distinct region of leakage power compared to the AND (e.g., AND+AND) and NAND (e.g., NAND+NOR) combinations. This separation of regions effectively creates three unique clusters separated into AND (lower-end), XNOR (middle-end), and NAND (high-end). This information could be a side channel, however, our study shows that the netlist with few camouflaged gates can obfuscate this signature. Since leakage power is additive in nature, for a full circuit. the total leakage of the circuit is the sum of leakage without camouflaging and the leakage of all the camouflaged gates. Hence, it follows that the full curcuit leakage behavior will show similar trends as in Fig. 17.

B. Delay Side Channel (for 3-input camouflaged gates)

Variations in temperature can reveal the camouflaged functionality of a circuit through path delay. An adversary can expose the circuit outside of normal operating temperatures to force a functional breakdown or determine some insights about the functionality. It can be seen previously from Fig. 11(a) that the delay profiles of NOR, XOR and XNOR are similar with respect to temperature. AOI and OAI configurations are also alike, and lower than the others. The NAND configuration is the most vulnerable as its delay significantly higher and sensitive to temperature. If the adversary has been able to separate out multiple instances of 3-input camouflaged gates, he can trigger a transition through a selected camouflaged gate and measure the output path delay by sweeping the temperature. At around 100C, a significantly high delay can identify the NAND functionality. Mid-range delays can identify one of AOI or OAI gates, and low-range delay can identify the remaining. By combining side channel information, the adversary can narrow down his search space and lower his RE effort.

C. Dynamic Power Consumption Side Channel

Active power consumption is another side channel signature for an adversary to profile the camouflaged gate to determine



(a) (b)

Fig. 17. Leakage power signature (2-input camouflaged gates) for (a) single gate instance; and, (b) combination of two gates.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

its functionality or narrow down search space. From Fig. 5(b) and Fig. 11(b), both 2-input and 3-input camouflaged gates show different power profiles per group of instances. Although at lower operating temperatures, the power profiles for the configurations are similar, the adversary can expose the circuit to high operating temperatures (above 100C), where high power consumption can identify cluster of gates by minimizing the group space. For example, 2-input camouflaged gates show that NOR, NAND, XNOR have similar profile while 3-input camouflaged gates show NAND and NOR have similar profile as temperature increases.

D. *Comparative Analysis of Gate and Interconnect Camouflaging*

We conducted comparative analysis of RE effort between gate and interconnect camouflaging technique (shown in Fig. 17). Mux-based interconnect camouflaging technique was found to offer the best RE effort only when mux became 8:1 or larger. Therefore, 3-function gate camouflaging technique should be used when the overhead is priority concern and interconnect camouflaging technique (8:1 mux or larger) should be used when the robustness is priority concern.

We also conducted comparative analysis of area, delay and power overheads for gate and interconnect camouflaging techniques (figures omitted for brevity). We used 3-function and 6-function gates for each metric. We noted that interconnect camouflaging using 2:1 mux resembles that of 3-function gate camouflaging technique in terms of area, delay and power overhead. The interconnect camouflaging using 2:1 mux is 5%, 9% and 8% better in terms of area, delay and power overhead respectively with respect to 6-function gate camouflaging while offering higher RE effort.

In regards to side-channel attacks, we have only shown the results for the gate camouflaging technique in this section. As shown in Fig. 17, our design provides higher resilience against side-channel attacks when a variety of gates are used to hide the signature. In contrast, interconnect camouflaging is not susceptible to side-channel attacks as the mux-based design is inherently symmetric with respect to the net selected/unselected by the LVT/HVT transistors, and thus, shows the same signature irrespective of the chosen net.

VII. Test-Chip Experimental Results [32]

A. *Test chip design*

The proposed camouflaging technique is experimentally evaluated by implemented in ST-Micro 65nm technology [32].

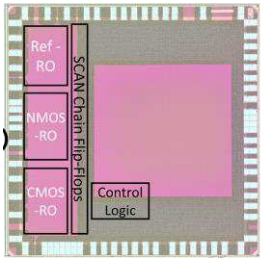


Fig. 18. Test-chip die image

The die-image with the design components (annotated) is shown in Fig. 18. The design is composed of three sets of 23 stage ring-oscillators (ROs). With one set being the reference (normal gate-based RO), the second set being the only NMOS-based (pass transistor) camouflaged gates and the third set being the full CMOS-based (transmission gate) camouflaged gates. Each set is composed of the six-logic function-based camouflaged RO. For example, the camouflaged gates are configured as NAND gates in the NAND-RO. Buffers are placed in-between each stage of RO to provide optimal swing. Additionally, the above sets (and ROs) are power-gated to ensure only the set being currently used is selected (turned ON). The output of all the sets are MUXed to a single output pin. The V_T switch voltage (V_{SN} and V_{SP}) are generated via a resistance ladder. A total of 8 voltages settings are present for both V_{SN} and V_{SP}, with V_{SN} ranging from 300mV to 650mV and V_{SP} ranging from 500mV to 850mV (for a supply voltage of 1.2V) with a 50mV step. *The V_T defined switches are enlarged to reduce process variation induced V_T shift*. The performance overheads as obtained from experimental data are shown in Table V.

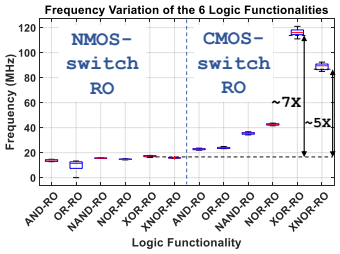


Fig. 19. Frequency distribution of 10 die for both the NMOS-switch and CMOS-switch based RO.

B. *Basic Setup*

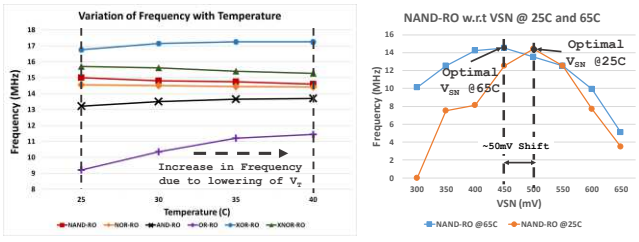
The experimental setup is composed of a logic analyzer (to scan in control data), a high-sampling oscilloscope and a dc-power supply. An oscilloscope is used to capture the oscillations of NMOS-switch based NAND camouflaged gate.

C. *Process Variations*

We have analyzed the frequency response of the NMOS and CMOS-switch based camouflaged gates for 10 test-chips (Fig. 19). We observe ~5% variation in the frequency distribution for each function. The designs exhibit less sensitivity to process variation due to the enlarged switches.

D. *Temperature Variations*

Fig. 20(a) illustrates the impact of temperature on the oscillation frequency of the NMOS switch-based RO. With the increase in temperature, the transistor's V_T reduces, which correspondingly shifts the HVT and LVT values. If left



(a) (b)

Fig. 20. (a) Variation of oscillating frequency under change in temperature for an NMOS-switch based RO; (b) Optimal VSN bias shift under the effect of temperature (65ºC).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

unchecked, the OFF switches with HVT will turn ON. This in turn will start contending with internal signals and corrupts the functionality. Therefore, V_{SN} and V_{SP} need to be adjusted appropriately to restore the optimal functionality. This is illustrated in Fig. 20(b), where the device is heated to a temperature of ~65ºC and the V_{SN} bias is swept from 300mV to 650mV to find the optimal bias point for a NMOS-based RO. It must be noted that the V_T of the device reduces by ~2mV for each degree rise in temperature, which would therefore shift the V_T of the device by ~80mV at 65ºC. From the experiment, we observe that the optimal V_{SN} bias point has shifted from 500mV at 25ºC to 450mV at 65ºC. This result indicates that bias voltage can be optimized to counter the effects of temperature. All modern processors include temperature sensors. The temperature and supply voltage combinations can be used to select appropriate V_{SN} and V_{SP} settings for the robust operation of the camouflaged gates.

VIII. CONCLUSION

In this paper, we proposed a V_T-defined camouflaged gates and a novel interconnect camouflaging technique to hide the functionality and connectivity information. By manipulating the threshold voltages of the transistors, the circuit is shown to configure itself to six different logic functions for different inputs, thereby hiding the true nature of the circuit from the adversary. In addition, by camouflaging interconnects, we maximize the adversarial RE effort with minimal overhead. Simulation as well as experimental test-chip results validate the effectiveness of our proposed approach.

ACKNOWLEDGEMENT

This work is supported by Semiconductor Research Corporation (SRC) (2727.001), National Science Foundation (NSF) (CNS-1722557, CCF-1718474, DGE-1821766 and DGE-1723687) and DARPA Young Faculty Award (D15AP00089)

REFERENCES

[1] F. Imeson, et al. "Securing computer hardware using 3D integrated circuit (IC) technology and split manufacturing for obfuscation." In 22nd USENIX Security Symposium, 2013.

[2] J. Rajendran, et al. "Security analysis of integrated circuit camouflaging." In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013.

[3] SypherMedia, "Syphermedia library circuit camouflage technology." http://www.smi.tv/solutions.htm

[4] Y. Wang, et al. "Retention time optimization for eDRAM in 22nm tri-gate CMOS technology." In 2013 IEEE International Electron Devices Meeting. 2013.

[5] R. Cocchi, et al. "Building block for a secure CMOS logic cell library." U.S. Patent 8,111,089, issued February 7, 2012.

[6] L. Chow, et al. "Camouflaging a standard cell based integrated circuit." U.S. Patent 8,151,235, issued April 3, 2012.

[7] R. Chakraborty, and S. Bhunia. "Hardware protection and authentication through netlist level obfuscation.", ICCAD, 2008.

[8] M. Rostami, F. Koushanfar, and R. Karri. "A primer on hardware security: Models, methods, and metrics." In *proc of the IEEE* 102, no. 8 (2014): 1283-1295.

[9] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri. "Security analysis of logic obfuscation." In Proceedings of DAC, 2012.

[10] A. Iyengar, and S. Ghosh. "Threshold Voltage-Defined Switches for Programmable Gates." GOMACTECH, 2015

[11] M. Mera, M. Massad, S. Garg. "Threshold-Dependent Camouflaged Cells to Secure Circuits Against Reverse Engineering Attacks" IEEE ISVLSI, 2016.

[12] X. Wang, et al. "Secure and Low-Overhead Circuit Obfuscation Technique with Multiplexer," in *proc of the 26th edition on* GLSVLSI'16, (Boston, MA, USA), pp. 133-136, ACM 2016.

[13] J. Rajendran, et al. "Regaining Trust in VLSI Design: Design-for-Trust Techniques." *Proc. of the IEEE*, 2014.

[14] M. Massad, et al. "Logic Locking for Secure Outsourced Chip Fabrication: A New Attack and Provably Secure Defense Mechanism" url: https://arxiv.org/abs/1703.10187 arXiv:1703.10187 [cs.CR]

[15] http://www.pld.ttu.ee/~maksim/benchmarks/iscas85/verilog

[16] A. Falk. "Advanced LIVA/TIVA Techniques." In ISTFA, pp. 59-68. ASM International; 1998, 2001.

[17] I. Nirmala et al. "A novel threshold voltage defined switch for circuit camouflaging." In 2016 21th IEEE ETS, pp. 1-2., 2016.

[18] Arizona State University 45nm Predictive Technology Model (PTM), http://ptm.asu.edu/modelcard/LP/45nm_LP.pm

[19] D. Lockhart. ECE5745. Tutorial, Topic: "RTL-to-Gates Synthesis using Synopsys Design Compiler". Cornell University, Jan. 30, 2016.

[20] A. De and S. Ghosh, "Preventing Reverse Engineering using threshold voltage defined multi-input camouflaged gates," In 2017 IEEE HST, Waltham, MA, 2017, pp. 1-6.

[21] L. Goldstein and E. Thigpen, "SCOAP: Sandia Controllability / Observability Analysis Program." *In Proc. of DAC*, 1980.

[22] C. Yu et al, "Incremental SAT-based Reverse Engineering of Camouflaged Logic Circuits," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2017.

[23] M. Li et al, "Provably secure camouflaging strategy for IC protection," in ICCAD, 2016, pp. 28:1–28:8.

[24] M. Yasin, et al., "CamoPerturb: Secure IC camouflaging for minterm protection," in Proc. ICCAD, 2016, pp. 29:1–29:8

[25] W. J. Dejka, "Measure of testability in device and system design," in *Proc. 20th Midwest Symp. Circuits Syst.*, Aug. 1977, pp. 39-52.

[26] L. Goldstein, "Controllability/observability analysis of digital circuits," in *IEEE Transactions on Circuits and Systems*, 26(9), Sep 1979.

[27] Muhammad Yasin, et. al, "Provably-Secure Logic Locking: From Theory To Practice" In Proceedings of ACM-CCS, 2017.

[28] S. Roshanisefat, H. M. Kamali, A. Sasan, "SRCLock: SAT-Resistant Cyclic Logic Locking for Protecting the Hardware. In Proc of the 2018 on Great Lakes Symposium on VLSI (GLSVLSI). pp. 153-158.

[29] B. Erbagci, et al., "A Secure Camouflaged Threshold Voltage Defined Logic Family," *IEEE HOST*, pp. 229-235, 2016.

[30] Akkaya, Nail Etkin Can, Burak Erbagci, and Ken Mai. "A secure camouflaged logic family using post-manufacturing programming with a 3.6 GHz adder prototype in 65nm CMOS at 1V nominal V DD." Solid-State Circuits Conference-(ISSCC), 2018

[31] Prashanth Mohan, Nail Etkin Can Akkaya, Burak Erbagci and Ken Mai. "A Compact Energy-Efficient Pseudo-Static Camouflaged Logic Family", HOST 2018.

[32] Anirudh Iyengar et al., "Threshold Defined Camouflaged Gates in 65nm Technology for Reverse Engineering Protection", in Proceedings of ISLPED, 2018.

[33] Chen, Shuai, et al. "Chip-level anti-reverse engineering using transformable interconnects." Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), 2015 IEEE International Symposium on. IEEE, 2015

[34] Patnaik, Satwik, et al. "Obfuscating the interconnects: Low-cost and resilient full-chip layout camouflaging." Computer-Aided Design (ICCAD), 2017 IEEE/ACM International Conference on. IEEE, 2017.

[35] K. Shamsi, et al, "Cross-Lock: Dense Layout-Level Interconnect Locking using Cross-bar Architectures," In Proc of the 2018 on Great Lakes Symposium on VLSI (GLSVLSI).

[36] D. Vontela and S. Ghosh, "Methodologies to exploit ATPG tools for de-camouflaging," *2017 18th International Symposium on Quality Electronic Design (ISQED)*, Santa Clara, CA, 2017, pp. 250-256.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2018.2887056, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

Jae-Won Jang received the B.Sc and the M.S from the University of South Florida (USF). Currently, he is working towards the Ph.D. degree in the department of Electrical and Computer Engineering (ECE) at the Virginia Polytechnic Institute. His research interests include Systems Security using Heterogeneous Architecture and Compilers.

Asmit De received his B. Tech degree in Computer Science and Engineering from National Institute of Technology Durgapur, India in 2014. He worked as a Software Engineer in the enterprise mobile security team at Samsung R&D Institute, India from 2014 to 2015. He is currently pursuing his PhD at PSU. His research interest is in developing secure hardware and architectures for emerging devices technologies.

Deepak Vontela received the M.Sc degree from the University of South Florida. His biography is not available at the time of publication

Ithihasa Nirmala received the M.Sc degree from the University of South Florida. Her biography and photography are not available at the time of publication

Swaroop Ghosh (Senior Member, IEEE) received the B.E. (honors) degree from the Indian Institute of Technology, Roorkee, India, in 2000, and the Ph.D. degree from Purdue University, West Lafayette, IN, USA, 2008. He joined Pennsylvania State University, University Park, PA, USA, in fall 2016. From 2012 to 2016, he was a Member of Faculty with USF. He was a Senior Research and Development Engineer with Advanced Design, Intel Corporation, from 2008 to 2012. His research interests include low-power circuit design and hardware security.

Anirudh Iyengar received the M.Sc. degree in electrical engineering from the University of South Florida, Tampa, FL, USA, 2013. In 2018, he received the Ph.D. degree in computer science and engineering at the Pennsylvania State University, State College, PA, USA, and currently working at Intel Corporation as a security researcher.
His research interests include low-power and secure circuits and systems.