Transistor-Level Camouflaged Logic Locking Method for Monolithic 3D IC Security

Jaya Dofe[1], Chen Yan[2], Scott Kontak[2], Emre Salman[2] and Qiaoyan Yu[1]

[1] Department of Electrical and Computer Engineering, University of New Hampshire, Durham, NH 03824, USA

[2] Department of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY 11794, USA

***Abstract*—This work proposes a novel method for transistor-level logic locking to address intellectual property (IP) piracy and reverse engineering attacks in monolithic three-dimensional (M3D) ICs. The proposed method locks logic gates by independently inserting parallel or serial locking transistors and camouflaged contacts in multiple tiers in M3D ICs. Without the correct key bits and confidential information for camouflaged contacts, the locked logic gates will malfunction and significantly alter power profiles, which makes reverse engineering attacks more difficult. The performance overhead of the proposed method is evaluated with ISCAS'85 benchmark circuits synthesized and placed with a customized M3D IC library. Case study on c6288 benchmark circuit shows that the proposed locking method with the correct key increases the power by only 0.26%. On average, this method consumes 2.3% more transistors than the baseline ISCAS'85 benchmark circuits.**

***Index Terms*—Hardware security, logic locking, logic encryption, reverse engineering, IP piracy, monolithic 3D ICs.**

I. Introduction

Integrated circuit (IC) trustworthiness emerges as a serious concern as the number of trusted foundries keeps decreasing [1]. The news, kill switches [2], hardware Trojan found in the Pentagon computers [3], and compromised hardware in commercial applications [4]–[6], all emphasize an imperative need of considering security perspective while developing future computational systems. Three-dimensional (3D) [7] ICs pave a new path to improve computation density, instead of increasing the transistor density of two-dimensional (2D) chips. The promising *monolithic 3D* (M3D) ICs eliminate the need for bulky through-silicon vias, wire bonding, interposer, and die-stack structure, and thus accelerate the speed of inter-tier communications in 3D computational systems. Despite the performance improvement, M3D technology leads to new security challenges [8], [9] over 2D ICs and 2.5/3D technologies.

Instead of targeting the security vulnerability in 3D ICs, existing security countermeasures involved in 3D ICs leverage 3D structure to address the security issues in untrusted 2D ICs. The stacked 3D ICs and 2.5/3D-packaging methods propose to split the entire system into multiple tiers, one tier per foundry [10]. Thus, a single foundry could not have the complete picture of the entire design. However in M3D IC fabrication, all tiers and vertical interconnects are manufactured by the same foundry, and thus splitting the system function to multiple tiers does not help to protect M3D ICs. Moreover, the reverse engineering and hardware intellectual property (IP) piracy attacks from untrusted testing entities, assembly parties, and unauthorized users will challenge the security of M3D ICs similar to 2D ICs.

This work investigates novel method to address the security challenges in M3D ICs. We propose a transistor-level logic locking method for M3D ICs to thwart reverse engineering and IP piracy attacks. Due to the limited availability of commercial 3D cell library, we develop a set of logic cells, schematic models and physical descriptions for HSPICE and Spectre simulation tools. The rest of this work is organized as follows. Section II introduces the related work, our 3D library development effort, and our contributions. Section III proposes a novel camouflaged logic locking method and proves the concept with an example. In Section IV, we evaluate our method in terms of output Hamming distance, power consumption profile over time, area overhead, and logic gate delay in several ISCAS'85 benchmark circuits. Section V concludes this work.

II. Related Work

A. Existing Logic Locking

Logic locking (or encryption) methods insert key-controlled logic gates in combinational circuits to alter the original logic function if a wrong key is applied. Without the correct key, it is extremely difficult for an attacker to reverse engineer the logic function (black box) based on the primary inputs and outputs. Lightweight logic encryption can be performed by adding XOR/XNOR gates to the original netlist [11]–[15]; an incorrect key bit may flip the primary output through XORing logic '1' or XNORing logic '0'. Alternatively, in multiplexer based logic encryption [12], [16], [17], multiplexers are inserted as key gates in the middle of logic paths. In addition to the original signal, another input for the key gate (i.e. multiplexer) is an arbitrary internal net. If the applied key is wrong, the multiplexer selects an arbitrary internal net for the primary output computation. Works [18], [19] suggest to implement logic gates as key-controlled lookup tables (LUTs), which unfortunately will incur significant area, power, and performance overhead. Recently, stack-based logic encryption topologies have been proposed to reduce per-gate overhead [20]. Those existing methods are all designed for 2D ICs. If these methods are applied to M3D ICs, attackers could use the same reverse engineering techniques developed for 2D

978-1-5090-5701-6/16/$31.00

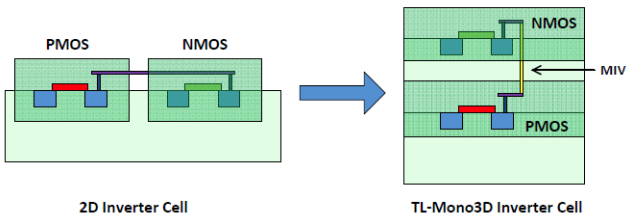

Fig. 1. **Transistor-level (TL) monolithic 3D integration design style, where all of the PMOS transistors are fabricated on one tier and all of the NMOS transistors are fabricated on the other tier [21].**

ICs to retrieve the key in 3D ICs. In this work, we exploit the unique characteristics of M3D ICs to perform multi-tier logic locking, where each tier can be locked independently.

B. Monolithic 3D ICs

M3D ICs enable ultra fine-grained vertical integration [22] since the monolithic inter-tier vias (MIVs) are fabricated using a similar process as the regular local metal vias. Multiple tiers for M3D ICs are fabricated sequentially by the same foundry. There are primarily three design styles for M3D ICs: block-level, gate-level, and transistor-level [23]. In our work, transistor-level *monolithic 3D* (TL-M3D) ICs are adopted. Through this style, the P-channel MOSFET (PMOS) and N-channel MOSFET (NMOS) within each standard cell are split into two different tiers connected by MIVs. In each TL-M3D standard cell, fabrication process for PMOS and NMOS are separately optimized. PMOS transistors are placed on the bottom tier and NMOS transistors are placed on the top tier due to high temperature processing steps. In this work, we developed a standard cell library for TL-M3D ICs [21] based on the baseline 2D standard cell library *FreePDK45* [24]. The process and physical characteristics for each 2D tier in the M3D standard cell library are retrieved from FreePDK45, including transistor models and physical characteristics (e.g. metal layer parameters and parasitic information).

C. Our Contributions

The main contributions of this work are as follows:

- To the best of our knowledge, this work is the first effort that studies logic locking for 3D ICs, more specifically for M3D ICs. Our method *places locking units in multiple tiers* ***independently***. Without the complete key sequence for all tiers, one leaked tier will not compromise the entire design. In contrast, the two portions of a complete circuit divided by split manufacturing have certain correlations, which may be exploited by attackers to accelerate the speed of reverse engineering the entire design.
- Unlike the existing logic encryption that locks combinational circuits with additional gates, our method locks a logic gate with a single transistor and camouflaged wires to power or ground grids. Four transistor-level camouflaged locking units are proposed to obfuscate pull-up or/and pull-down networks in logic gate cells. An incorrect key will not only lead to a flipped output logic value, but could also result in either a floating ground/power pin or a shorted ground/power line. As our method increases the diversity of the consequences caused by incorrect unlocking, it is more difficult for attackers to succeed in reverse engineering and IP piracy.

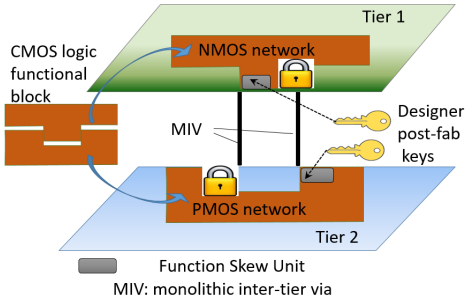

Fig. 2. **Proposed transistor-level camouflaged logic locking mechanism for M3D ICs against reverse engineering and IP piracy attacks.**

III. Proposed Transistor-Level Camouflaged Logic Locking Method

A. Method Overview

We propose a multi-tier logic locking mechanism for M3D ICs to thwart reverse engineering attacks and IP piracy. We assume that the attacker may use image-analysis based reverse engineering techniques and primary outputs to retrieve the original circuit design (black box). As shown in Fig. 2, a functional block is fabricated in two tiers, PMOS pull-up network (PUN) on the bottom tier and NMOS pull-down network (PDN) on the top tier. PUN and PDN on different tiers are independently locked by the proposed camouflaged locking circuit. **The number of locking units, key values, and locking circuit locations for two tiers are different**. This arrangement protects the 3D circuit from attacks that try to exploit the collaborative analysis on two tiers. An invalid key applied to the locked functional block either leads to malfunctions or/and significant changes on the power profile. The locking keys are only available to authorized users. Even if the complete layout is available to adversary, it would still be highly challenging for attackers to reverse engineer the entire locked 3D circuit. Our locking unit can be inserted with parallel or serial locking configuration. In total, we propose four locking configurations: PMOS parallel locking (**PPL**), NMOS parallel locking (**NPL**), PMOS serial locking (**PSL**), and NMOS serial locking (**NSL**).

B. Serial 3D Logic Locking

The concept of the proposed serial locking circuit is depicted in Fig. 3. The PMOS transistor (*P1*) is controlled by a key bit (*Key1*). The power pin VDD and the *P1* source terminal are connected with PUN through camouflaged contacts. One of the camouflaged contacts is filled with dielectric, which results in only one real connection. As demonstrated in 2D ICs, contact camouflaging is feasible and promising to thwart image-analysis-based reverse engineering attacks [25]. The locking circuit can also be applied to the PDN tier, where a

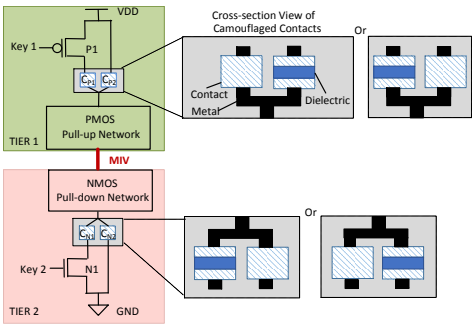

Fig. 3. **Proposed 3D logic cell with serial locking (PSL and NSL) against reverse engineering attacks.**

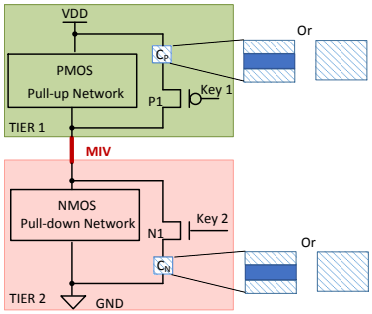

Fig. 4. **Proposed 3D logic cell with parallel locking (PPL and NPL) against reverse engineering attacks.**

TABLE I
CONTACT AND TRANSISTOR STATUS IN SERIAL LOCKING

		Correct	**Key1,**	**Key2**	**= 0**		
Key	C_{N1}	C_{N2}	C_{P1}	C_{P2}	$N1$	$P1$	Result
0	X	✓	✓	X	off	on	normal
1	X	✓	✓	X	on	off	**floating VDD**

		Correct	**Key1,**	**Key2**	**= 1**		
Key	C_{N1}	C_{N2}	C_{P1}	C_{P2}	$N1$	$P1$	Result
0	✓	X	X	✓	off	on	**floating GND**
1	✓	X	X	✓	on	off	normal

TABLE II
CONTACT AND TRANSISTOR STATUS IN PARALLEL LOCKING

		Correct	**Key1,**	**Key2 = 0**	
Key	C_N	C_P	$N1$	$P1$	Result
0	✓	X	off	off	normal
1	✓	X	on	off	**always pull-down**

		Correct	**Key1,**	**Key2 = 1**	
Key	C_N	C_P	$N1$	$P1$	Result
0	X	✓	off	off	**always pull-up**
1	X	✓	off	off	normal

NMOS locking together with a short-circuit wire are inserted between the NMOS PDN and the real ground line. Different *Key1* and *Key2* will help to reduce the correlation between tier 1 and tier 2. For simplicity, we use the same value for *Key1* and *Key2* in the following example. Table I lists the connection configuration for the camouflaged contacts C_{N1}, C_{N2}, C_{P1}, and C_{P2} for different key value scenarios. In the first half of Table I, the real design setting is as follows: the correct key bit is 0, the contacts C_{N1} and C_{P2} are disconnected with dielectric, only C_{N2} and C_{P1} are truly connected. The hypothesis key of 1 will turn off PMOS $P1$, thus causing a floating VDD. Figure 3 depicts this scenarios. The second half of Table I shows another configuration if the correct key bit is 1. In this case, the camouflaged contacts C_{N2}, C_{P1} are not truly connected. The wrong hypothesis key of 0 will turn off NMOS $N1$ and cause PDN to have a floating ground. To implement this configuration, the camouflaged contacts in Fig. 3 need to be modified.

C. Parallel 3D Logic Locking

Alternatively, the proposed camouflaged logic locking can be performed in parallel with the original PDN and PUN, as shown in Fig. 4. Contrary to the serial locking circuit, no short-circuit wire is needed in parallel locking. If the correct key is 0 (the first half of Table II), the contact C_N is truly connected but the contact C_P is disconnected in the camouflaged layout. Because of the camouflaged disconnection in C_P, the wrong key bit (i.e. 1) produces a pull-down network always shorted to ground. The second half of Table II indicates that the camouflaged disconnection in C_N will cause the pull-up network always shorted to VDD if the wrong key of 0 is applied to $P1$.

Figures 3 and 4 show that a single transistor is used in locking units. In real designs, the locking circuits for PUN and PDN are not necessarily symmetric. Asymmetric locking circuit will provide stronger protection against reverse engineering attacks. Our method is particularly designed to prevent the attacker from correlating PUN and PDN after the separation of the PMOS and NMOS tiers. Our ultimate goal is to thwart attackers from understanding the entire 3D IC design. Even if the attacker retrieves the design of one tier, it is still difficult to completely derive the design in another tier.

D. Proof of Concept

We used our monolithic cells to implement an ISCAS'85 benchmark circuit, c17. The VDD of one NAND2X1 gate in c17 is locked by PSL shown in Fig. 5(a). Camouflaged contacts are applied in the PDN of that same NAND2X1 gate. As the NMOS locking transistor is shorted to ground (via C_{N2} contact, we omit the locking circuit in Fig. 5(a)). When the key bit is low, the PMOS is turned on and thus c17 operates normally. Figure 5(b) shows the impact of key on the c17 primary outputs and power. The input patterns for valid and invalid key period are exactly the same. However, the primary outputs, N22 and N23, yield different values for invalid and valid key scenarios. The corresponding power profiles for valid and invalid key periods are also different. This example demonstrates that the circuit locked by key bits through PSL indeed alters the primary outputs and power profile, thus obscuring the 3D circuit if the attacker does not have the valid key.

We repeated the experiment by replacing PSL with PPL. The corresponding output signals and power profile are shown in Fig. 5(c). Compared to Fig. 5(b), the consequence of always

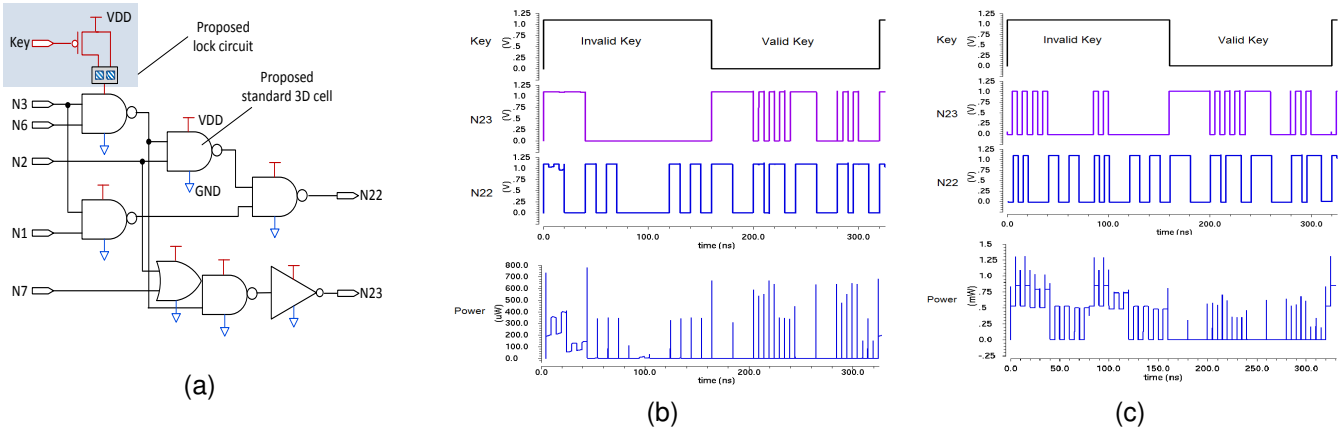

Fig. 5. **(a) Schematic for locked c17 circuit, and impact of invalid/valid key on output signals and power of the (b) serial and (c) parallel locked c17.**

pull-down caused by an incorrect key leads to a significant change on power, which does not match to the power profile for any logic gate. Thus, the proposed locking circuit can also resist power-based side-channel attacks.

IV. Experimental Results

A. Experimental Setup

Our simulations in this section is based on our M3D standard cell library. We used Calibre from Mentor Graphics to perform M3D standard library physical verification steps, which include design rule check (DRC), layout versus schematic (LVS) and parasitics extraction (PEX). The Calibre DRC, LVS and PEX (including MIV parasitic impedances) rules were modified based on the rule files provided with FreePDK45 [24]. Library liberty file which contains the timing and power information for each cell was generated by Cadence Encounter Library Characterizer. The FreePDK45 technology was used to develop a library for synthesis and schematic design of 3D logic cells and four locking circuits. ISCAS'85 benchmark circuits were first synthesized in Synopsys Design Vision with our 3D library. Next, locking circuit cells were inserted into the synthesized netlists in the same way shown in Figs. 3 and 4. Then, the modified netlists were imported to Cadence Virtuoso for transistor-level simulation. Random inputs were provided for each benchmark circuit.

B. Power Comparison

1) Impact of Different Logic Locking Styles on Power: We used Cadence Virtuoso Spectre simulator to perform power consumption comparison among the 3D baseline c432 and its four locking configurations. Five logic gates were selected to lock with each locking configuration. We sampled the power profile with a sampling frequency of 1GHz. Figure 6(a) shows the differential power between locked and baseline c432 circuits. As shown by this figure, the increase in power consumption due to parallel locking is three orders of magnitude higher than the increase in power due to serial locking. From c880 power comparison shown in Fig. 6(b), we can observe a similar power impact. Thus, in the rest of Section IV-B, we use

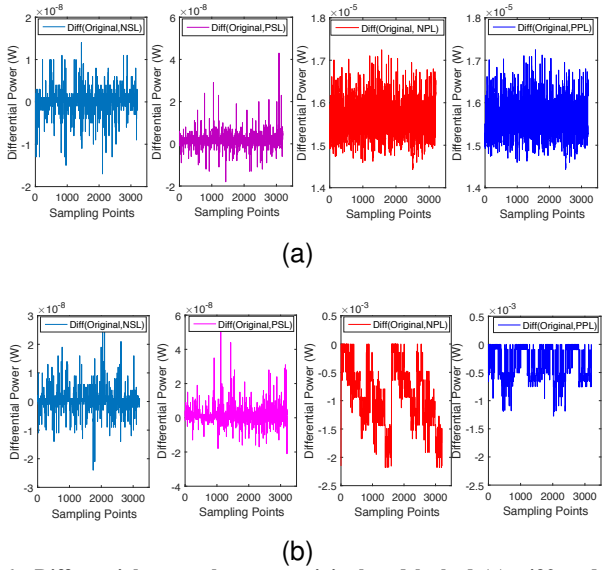

Fig. 6. **Differential power between original and locked (a) c432 and (b) c880 benchmark circuits.**

parallel locking, *PPL*, as an example to further demonstrate the impact of locking circuits on power.

2) Power Overhead Induced by Locking Circuit: Table III lists the average power (including dynamic and static power) consumption for different ISCAS'85 benchmark circuits protected with different locking configurations. *Baseline* configuration represents no protection. *5-bit locking* refers to the case where five logic gates were randomly chosen and locked with PPL circuit. *Fully locking* means locking every gate in the circuit. *wk* and *ck* stand for wrong key and the correct key, respectively. As indicated in Table III, the use of locking circuit will increase the power consumption compared to the baseline circuit. Generally, more gates protected by locking units will result in a higher power overhead. The configuration of 5-bit locking *wk* yields a power overhead over 150%. Fully locking *wk* cases lead to more than 3.5× power consumption. However, if the correct key is applied to the locked circuit, the power overhead of fully locking *ck* is much less than the case

TABLE III
POWER OVERHEAD INDUCED BY DIFFERENT PPL LOCKING.
(UNIT: W; WK: WRONG KEY APPLIED, CK: CORRECT KEY APPLIED)

Circuits (No. Syn. Gates)	**c432** (185)	**c880** (280)	**c1908** (286)	**c1355** (391)	**c6288** (2115)
Baseline	111.1μ	267.2μ	411.2μ	605.4μ	$4.616m$
5-bit locking wk	497.3μ	606.2μ	1.002μ	966.1μ	$7.251m$
Fully locking wk	$8.527m$	$9.802m$	$13.52m$	$10.33m$	$16.22m$
Fully locking ck (power increase over Baseline)	166.9μ (50.2%)	301.1μ (12.7%)	445.5μ (8.3%)	628.7μ (3.8%)	$4.628m$ (0.26%)

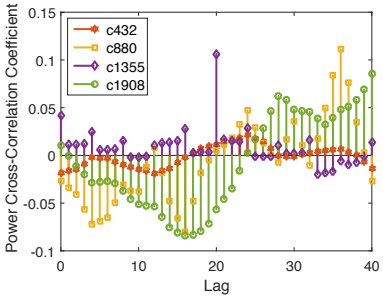

Fig. 7. **Cross-correlation coefficient between the sampled power sequences of locked circuits with and without correct key.**

using a wrong key. As shown in the last row of Table III, the fully locking *ck* case increases the average power by 50.2% for a small circuit c432. However, the power overhead decreases as the circuit scale increases. The fully locking *ck* for c6288 only introduces 0.26% power increase over the baseline.

3) Power Cross-Correlation Coefficient: In this subsection, we zoom in the power consumption to study the cross correlation between the power profiles of the circuit unlocked with the correct key and one wrong key. If two sampled power sequences are correlated (i.e. the cross-correlation coefficient is close to 1 at one of the lag values), the guessed locking key is close to the correct locking key. We randomly chose a key sequence for every 100 random input patterns, and sampled the power sequences for c432, c880, c1355 and c1908 circuits with the sampling frequency of 1GHz. We used the *crosscorr* function in MATLAB to calculate the cross-correlation coefficient between the power profiles of the circuits with and without the correct key. As shown in Fig. 7, the cross-correlation coefficient for different benchmark circuits with proposed locking circuit is nearly in the range of +/-0.1. This result indicates that our method is promising to thwart power-based side-channel attacks, as a minor error on the key will lead to a significant change on power.

4) Impact of Locking Unit Location on Power: Figure 8 shows the impact of locking unit location on the power consumption of c432. To save hardware cost, one may selectively lock the circuit with our locking configurations. According to Fig. 8, even using the same key length, it is necessary to search for the best location for key insertion to maximize the power difference between the correct and wrong key scenarios.

C. Hamming Distance of Primary Outputs

Another notable impact of a wrong key on a locked circuit is malfunction. Hamming distance (HD) is adopted as a metric

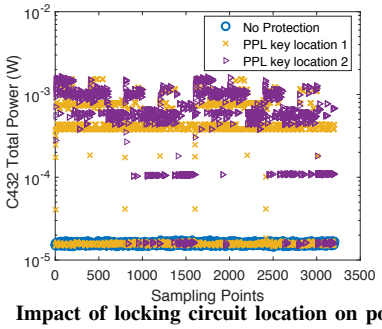

Fig. 8. **Impact of locking circuit location on power.**

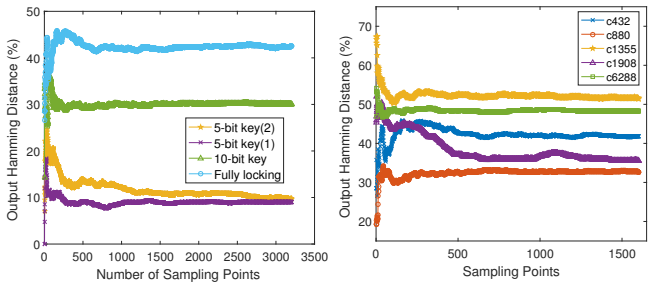

Fig. 9. **Hamming distance for the primary outputs of (a) c432 with correct and incorrect locking key and (b) other benchmark circuits.**

to evaluate the difference between the primary outputs from the circuit unlocked with the valid key and a wrong key. The ideal output HD is 50% [12], which indicates the maximum output difference achieved by the locking circuit.

We used c432 as a case study, in which we first randomly selected two sets of five gates for PPL locking. As shown in Fig. 9(a), the same key length eventually leads to nearly same output HD. Then, we extended the key length to 10 bits by locking five more gates. The output HD is improved to 30%. When we added the locking circuit to every gate in c432 (i.e. fully locking), the output HD reaches 42.5%.

We further examined the output HD of other benchmark circuits. Since the HD is stabilized after 1600 sampling points, we shorten the simulation time to 1.6μs. The trend of HD for other circuits is shown in Fig. 9(b). As can be seen, our method achieves HD in the range of 35.74% to 52.09%, which approaches to the ideal 50% HD. In future work, we will exploit the techniques proposed in [12], [16] to improve our HD.

D. Hardware Cost Comparison

We completed the layout of 3D 2-input NAND (baseline) and added the proposed locking configurations, respectively. We used 1.1V VDD, $27°C$ temperature, typical process corner, 1GHz input switching frequency, and 20ns total simulation period in our HSPICE simulation. The area, delay, current, and total power consumption are reported in Table IV. Our locking circuit increases the layout area by 20% as compared to the baseline. The delay overhead induced by different locking configuration is in the range of 5.6% and 21.8%. We further compared the overhead of our locking method with the

TABLE IV
HARDWARE COST AND PERFORMANCE COMPARISON OF 3D NAND2 GATE W/WO PROPOSED FOUR LOCKING CIRCUITS

Lock Configuration	Baseline	PSL	PPL	NSL	NPL
Layout Area (μm^2)	0.681	0.8172	0.8172	0.8172	0.8172
Gate Delay (ps)	9.4841	11.301	11.547	10.018	10.881
Avg. Current (μA)	2.0097	1.7788	2.2283	1.7078	2.1061
Total Power (μW)	2.2107	1.9567	2.4511	1.8786	2.3167

TABLE V
COMPARISON OF PER-GATE OVERHEAD OVER BASELINE

Methods	Delay overhead	Power overhead	Area overhead
XOR-based [13]	247.6%	95.7%	174.1%
LUT-based [18]	239.4%	116.0%	289.6%
Stack-based [20]	168.4%	39.0%	119.8%
Proposed	21.8%	10.9%	20.0%

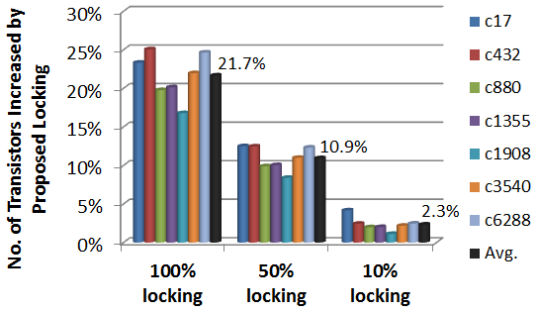

Fig. 10. **Number of transistors increased by 100%, 50% and 10% locking.**

XOR-based [13], LUT-based [18], and stack-based [20] logic encryption methods in Table V. The overhead of our method is based on Table IV. The overhead of other NAND gates over an non-encrypted NAND were calculated based on the results reported in [20]. As shown in Table V, our method reduces the gate delay, power, and area overhead by 146.6%, 28.1%, and 99.8%, respectively, than the most efficient locking method.

Moreover, the increase on area and delay for a single logic cell does not necessarily equal to the same overhead for the entire circuit under protection. Depending on hardware budget, a defender can determine the percentage of circuits for the proposed logic locking. We calculated the number of transistors that is needed for baseline and 100%, 50%, and 10% PPL locking. As shown in Fig. 10, if we lock 50% of the logic gates in the circuit, the number of transistors (on average) will increase by 10.9%. This overhead can be further reduced to 2.3% if we lock 10% of the target circuit.

V. CONCLUSION

The emergence of *monolithic 3D* ICs leads to new security challenges due to offshore fabrication, untrusted testing and assembly entities. This work proposes four transistor-level logic locking circuits, which will cause logic malfunctions by opening or shorting pull-up or pull-down network if a wrong locking key is applied. We further exploit contact camouflaging to thwart image-analysis based reverse engineering, and provide a novel way to lock PMOS or/and NMOS tiers independently for M3D ICs. HSPICE simulation on 3D NAND gate (at the layout level) shows that the proposed locking mechanism reduces the gate delay overhead, power overhead, and area overhead by 146.6%, 28.1%, and 99.8%, respectively, than the most efficient logic encryption methods. The proposed locking circuits have been successfully applied to ISCAS'85 benchmark circuits. For c6288, the proposed method increases the average power by only 0.26% than the baseline. On average, our method increases the transistor overhead by 21.7%, 10.9% and 2.3% for 100%, 50% and 10% locking, respectively. In future work, we will investigate methods to maximize Hamming distance while minimizing lock circuits.

REFERENCES

[1] "World Semiconductor Trade Statistics, 2011 Blue Book," 2012. https://www.wsts.org/content/download/2395/16194.

[2] S. Adee, "The Hunt For The Kill Switch," *IEEE Spectrum*, vol. 45, pp. 34–39, May 2008.

[3] J. Markoff, "FBI says the military had bogus computer gear," *New York Times (May 9, 2008), http://www.nytimes.com*, 2008.

[4] "Dell warns of hardware Trojan," July 21, 2010. http://www.homelandsecuritynewswire.com/dell-warns-hardware-trojan.

[5] J. Dastin, "Computer glitch halts United Airlines flights for two hours," *http://www.reuters.com*, 2015.

[6] N. Popper, "The stock market bell rings, computers fail, wall street cringes," *New York Times (July 8, 2015), http://www.nytimes.com*, 2015.

[7] S. Panth, S. Samal, Y. S. Yu, and S. K. Lim, "Design challenges and solutions for ultra-high-density monolithic 3D ICs," in *Proc. S3S'14*, pp. 1–2, Oct 2014.

[8] J. Dofe, Q. Yu, H. Wang, and E. Salman, "Hardware security threats and potential countermeasures in emerging 3D ICs," in *Proc. GLSVLSI*, pp. 69–74, May 2016.

[9] P. Gu, et al., "Leveraging 3D Technologies for Hardware Security: Opportunities and Challenges," in *Proc. GLSVLSI*, pp. 347–352, 2016.

[10] F. Imeson, A. Emtenan, S. Garg, and M. Tripunitara, "Securing Computer Hardware Using 3D Integrated Circuit (IC) Technology and Split Manufacturing for Obfuscation," in *USENIX*, pp. 495–510, 2013.

[11] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Security analysis of logic obfuscation," in *Proc. DAC'12*, pp. 83–89, June 2012.

[12] J. Rajendran, et al., "Fault Analysis-Based Logic Encryption," *IEEE Transactions on Computers*, vol. 64, pp. 410–424, Feb 2015.

[13] J. Roy, F. Koushanfar, and I. Markov, "EPIC: Ending Piracy of Integrated Circuits," in *Proc. DATE'08*, pp. 1069–1074, March 2008.

[14] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Logic encryption: A fault analysis perspective," in *Proc. DATE'12*, pp. 953–958, 2012.

[15] O. Sinanoglu, Y. Pino, J. Rajendran, and R. Karri, "Systems, processes and computer-accessible medium for providing logic encryption utilizing fault analysis," Dec. 25 2014. US Patent App. 13/735,642.

[16] S. M. Plaza and I. L. Markov, "Solving the Third-Shift Problem in IC Piracy With Test-Aware Logic Locking," *TCAD*, vol. 34, pp. 961–971, June 2015.

[17] J. B. Wendt and M. Potkonjak, "Hardware obfuscation using PUF-based logic," in *Proc.ICCAD'14*, pp. 270–271, Nov 2014.

[18] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC Piracy Using Reconfigurable Logic Barriers," *IEEE Design Test of Computers*, vol. 27, pp. 66–75, Jan 2010.

[19] B. Liu and B. Wang, "Reconfiguration-based VLSI design for security," *ETCAS*, vol. 5, pp. 98–108, March 2015.

[20] K. Juretus and I. Savidis, "Reduced overhead gate level logic encryption," in *Proc. GLSVLSI'16*, pp. 15–20, 2016.

[21] H. Wang, *Enhancing Signal and Power Integrity in Three-Dimensional Integrated Circuits*. PhD thesis, Stony Brook University, 2016.

[22] S. A. Panth, K. Samadi, Y. Du, and S. K. Lim, "Design and CAD Methodologies for Low Power Gate-level Monolithic 3D ICs," in *Proc. ISLPED'14*, pp. 171–176, ACM, 2014.

[23] S. Panth, S. K. Samal, Y. S. Yu, and S. K. Lim, "Design Challenges and Solutions for Ultra-High-Density Monolithic 3D ICs.," *J. Inform. and Commun. Convergence Engineering*, vol. 12, no. 3, pp. 186–192, 2014.

[24] "FreePDK45 [online]." http://www.eda.ncsu.edu/wiki/NCSU_EDA_Wiki.

[25] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security Analysis of Integrated Circuit Camouflaging," in *Proc. CCS'13*, pp. 709–720, 2013.